9.3

IBM MQ v kontejnerech

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 215.

Toto vydání se vztahuje na verzi 9 vydání 3 produktu IBM® MQ a na všechna následná vydání a úpravy, není-li v nových vydáních uvedeno jinak.

Obsah

Multi IBM MQ v kontejnerech a IBM Cloud Pak for Integration

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

Můžete spustit IBM MQ pomocí IBM MQ Operator v systému Red Hat® OpenShift®. To lze provést pomocí IBM Cloud Pak for Integration, IBM MQ Advanced nebo IBM MQ Advanced for Developers.

Produkt IBM MQ můžete také spustit v kontejneru, který sami sestavujete.

MQ Adv. CD Další informace o IBM MQ Operator viz následující odkazy.

Multi 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 produktu IBM MQ v architektuře kontejnerů byste se měli seznámit se základními koncepty produktu IBM MQ (viz téma IBM MQ Technický přehled) a základními koncepty Kubernetes/Red Hat OpenShift (viz téma OpenShift Container Platform architektura).

Procedura

- “Zvolení, jak se má produkt IBM MQ používat v kontejnerech” na stránce 5.
- “Podpora pro IBM MQ v kontejnerech” na stránce 6.
- “Aspekty úložiště pro IBM MQ Operator” na stránce 20.
- “Vysoká dostupnost pro IBM MQ v kontejnerech” na stránce 25.
- “Zotavení z havárie pro produkt IBM MQ v kontejnerech” na stránce 27.
- “Ověření uživatele a autorizace pro produkt IBM MQ v kontejnerech” na stránce 28.

Zvolení, jak se má produkt IBM MQ používat v kontejnerech

Existuje více voleb pro použití produktu IBM MQ v kontejnerech: můžete zvolit použití IBM MQ Operator, který používá předem seskupené kontejnerové obrazy nebo můžete sestavit vlastní obrazy a kód implementace.

Použití produktu IBM MQ Operator

OpenShift CP4I

Plánujete-li implementovat v produktu Red Hat OpenShift Container Platform, pravděpodobně budete chtít používat IBM MQ Operator.

Produkt IBM MQ Operator rozšiřuje rozhraní API Red Hat OpenShift Container Platform a přidává nový vlastní prostředek `QueueManager` . Operátor sleduje nové definice správce front a poté je změní na nezbytné prostředky s nízkou úrovní, jako například prostředky `StatefulSet` a `Service`. V případě nativní vysoké dostupnosti může operátor také provést komplexní průběžnou aktualizaci instancí správce front. Viz “Faktory ovlivňující provádění vlastní průběžné aktualizace správce front nativní vysoké dostupnosti” na stránce 211

Některé funkce IBM MQ nejsou podporovány při použití IBM MQ Operator. Podrobnosti o tom, co je podporováno při použití konzoly IBM MQ Operator, naleznete v části “Podpora pro IBM MQ v kontejnerech” na stránce 6 .

Všimněte si, že produkt IBM MQ Operator nepodporuje instalaci na klastr OpenShift s výpočetními počítači s více architekturami.

Vytváření vlastních obrazů a kódu implementace

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 a kódu implementace” na stránce 203.

Podrobnosti o tom, co je podporováno při sestavování vlastního obrazu a kódu implementace, naleznete v části “Podpora pro IBM MQ v kontejnerech” na stránce 6 .

Související odkazy

“Podpora pro IBM MQ v kontejnerech” na stránce 6
Ne všechny funkce produktu IBM MQ jsou k dispozici a podporovány stejným způsobem v kontejnerech.

Podpora pro IBM MQ v kontejnerech

Ne všechny funkce produktu IBM MQ jsou k dispozici a podporovány stejným způsobem v kontejnerech.

Níže je uvedena tabulka, která podrobně zobrazuje, jak jsou funkce produktu IBM MQ podporovány s produktem IBM MQ Operator, nebo když sestavujete vlastní kontejnery a kód implementace.

Poznámka: Předem sestavené obrazy kontejneru IBM MQ v systému IBM Container Registry (icr.io a cp.icr.io) jsou podporovány a vhodné pro opravy, pokud se používají s produktem IBM MQ Operator.

Není možné "upgradovat" licenci předem sestaveného obrazu IBM MQ Advanced for Developers na jinou licenci. Produkt IBM MQ Operator nasadí různé obrazy v závislosti na tom, která licence je vybrána.

V této tabulce platí následující podmínky:

"Kód povolení kontejneru"
: Spustitelné soubory **runmqserver**, **runmqintegrationserver**, **chkmqhealthy**, **chkmqready** a **chkmqstarted**. Tento kód je poskytován jako ukázka a je podporován pouze jako součást předem sestavených kontejnerů při použití s produktem IBM MQ Operator.

	Použití produktu IBM MQ Operator a IBM Cloud Pak for Integration licence	Použití produktu IBM MQ Operator a IBM MQ Advanced licence	Použití produktu IBM MQ Operator a IBM MQ Advanced for Developers licence	Předsestavený IBM MQ Advanced for Developers obraz	Sestavte-svůj-vlastní kontejner
podporované platformy	Podporováno pouze na systému Red Hat OpenShift Container Platform . Verze produktu Red Hat OpenShift Container Platform již nejsou podporovány IBM MQ jednou Red Hat zastavením podpory. Další podrobnosti viz “Podpora verze pro IBM MQ Operator” na stránce 11.		K dispozici pouze v systému Red Hat OpenShift Container Platform , ale není podporováno.	Pracuje na libovolné platformě Docker, containerd nebo cri-o, ale není podporováno. Podrobnosti lze najít v tématu Systémové požadavky pro IBM MQ.	Libovolná platforma Docker, containerd nebo cri-o. Podrobnosti lze najít v tématu Systémové požadavky pro IBM MQ. Nativní vysoká dostupnost je podporována pouze v systému Kubernetes nebo Red Hat OpenShift Container Platform. Ukázkový obraz kontejneru používá technologii Red Hat Universal Base Image (UBI), která zahrnuje knihovny a obslužné programy systému Linux® používané produktem IBM MQ. UBI je podporován společností Red Hat při spuštění v Red Hat OpenShift. *Kód pro povolení kontejneru* není podporován.
Architektury CPU	Podporováno na systémech `amd64`, `s390x` z/Linuxa `ppc64le` Power Systems.		K dispozici na systémech `amd64`, `s390x` z/Linuxa `ppc64le` Power Systems, ale není podporováno.		Podle softwaru IBM MQ .

	Použití produktu IBM MQ Operator a IBM Cloud Pak for Integration licence	Použití produktu IBM MQ Operator a IBM MQ Advanced licence	Použití produktu IBM MQ Operator a IBM MQ Advanced for Developers licence	Předsestavený IBM MQ Advanced for Developers obraz	Sestavte-svůj-vlastní kontejner
Doba trvání podpory	IBM Cloud Pak for Integration - Long Term Support nebo Continuous Delivery.[1] Operátor CD a správci front jsou podporováni až do dalšího vydání produktu IBM Cloud Pak for Integration CD nebo CP4I-LTS . Operátor CP4I-LTS a správci front jsou podporováni až do dalšího vydání produktu IBM Cloud Pak for Integration CP4I-LTS spolu s dobou odkladu, která umožňuje přechod na vyšší verzi.	Pouze proud Continuous Delivery pro správce front i IBM MQ Operator. Každá verze produktu IBM MQ Operator a správce front je podporována pouze do dalšího vydání CD nebo LTS .	Nepodporováno		Podle softwaru IBM MQ . Viz téma IBM MQ Často kladené dotazy pro vydání Long Term Support a Continuous Delivery. *Kód pro povolení kontejneru* není podporován.

[1] Produkt IBM MQ Operator je podporován buď jako vydání produktu IBM MQ CD , nebo jako vydání produktu CP4I-LTS :

- IBM MQ 9.3.0.x obrazy kontejneru implementované s produktem IBM MQ Operator 2.0.x, jsou-li použity jako součást produktu IBM Cloud Pak for Integration 2022.2.1, jsou vhodné pro podporu produktu CP4I-LTS . Nejnovější verze produktu IBM MQ Operator Long Term Support (LTS) je 2.0.23a nejnovější obraz kontejneru LTS je 9.3.0.17-r3.
- IBM MQ 9.3.5 obrazy kontejneru implementované s produktem IBM MQ Operator 3.1.x, jsou-li použity jako součást produktu IBM Cloud Pak for Integration 2023.4.1, jsou vhodné pro podporu produktu CD . Nejnovější verze produktu IBM MQ Operator Continuous Delivery (CD) je 3.1.3a nejnovější obraz kontejneru CD je 9.3.5.1-r2.

	Použití produktu IBM MQ Operator a IBM Cloud Pak for Integration licence	Použití produktu IBM MQ Operator a IBM MQ Advanced licence	Použití produktu IBM MQ Operator a IBM MQ Advanced for Developers licence	Předsestavený IBM MQ Advanced for Developers obraz	Sestavte-svůj-vlastní kontejner
Dostupnost oprav zabezpečení	Pravidelné opravy dostupné jako obrazy kontejnerů na IBM Container Registry				Opravy softwaru IBM MQ jsou k dispozici jako software na systému Fix Central. *Kód pro povolení kontejneru* není podporován.
Dostupnost prozatímní opravy	Opravy správce front dostupné jako software a vlastní sestavení obrazu je nezbytné. IBM MQ Operator opravy nejsou k dispozici jako prozatímní opravy.		Nejsou k dispozici žádné prozatímní opravy.		Opravy softwaru IBM MQ jsou k dispozici jako software na systému Fix Central nebo prostřednictvím podpory IBM . *Kód pro povolení kontejneru* není podporován.
Funkce: Advanced Message Security	Podporováno. Všimněte si, že není snadné použít šifrování na straně serveru, protože IBM MQ Operator přímo neumožňuje zadat vlastní úložiště klíčů pro Advanced Message Security.		K dispozici, ale není podporováno.		Podporováno podle softwaru IBM MQ , ale není k dispozici žádný vzorek.
Funkce: Managed File Transfer	Není k dispozici a není podporováno. Produkt IBM MQ Operator však můžete použít k poskytnutí jednoho nebo více správců front Coordination, Command nebo Agent.			Není k dispozici a není podporováno.	Podporováno podle softwaru IBM MQ , s ukázkou pro agenta.
Funkce: MQTT	Není k dispozici a není podporováno.				Podporováno podle softwaru IBM MQ , ale není k dispozici žádný vzorek.
Funkce: AMQP	Není k dispozici a není podporováno.				Podporováno podle softwaru IBM MQ , ale není k dispozici žádný vzorek.

	Použití produktu IBM MQ Operator a IBM Cloud Pak for Integration licence	**Použití produktu IBM MQ Operator a IBM MQ Advanced licence**	**Použití produktu IBM MQ Operator a IBM MQ Advanced for Developers licence**	**Předsestavený IBM MQ Advanced for Developers obraz**	**Sestavte-svůj-vlastní kontejner**
Funkce: REST API	Dostupné a podporované od IBM MQ Operator 3.0 a IBM MQ 9.3.4 dále. Dříve nebyla podporována rozhraní REST API.	K dispozici a podporováno. Snadná konfigurace od verze IBM MQ Operator 3.0 a IBM MQ 9.3.4 dále.	Dostupné a podporované od verze IBM MQ Operator 3.0 a IBM MQ 9.3.4 , ale nepodporované . Dříve nebyla rozhraní REST API k dispozici.	Dostupné a podporované od verze IBM MQ 9.3.4 dále, ale nepodporované . Před tím nebyl produkt REST API k dispozici.	K dispozici a podporováno podle softwaru IBM MQ .
Funkce: Správci front replikovaných dat	Není k dispozici a není podporováno. Správci front replikovaných dat jsou úzce spojeni s jádrem Linux a nejsou podporováni v kontejnerech.				
Funkce: Nativní HA	K dispozici a podporováno.		K dispozici, ale není podporováno.		K dispozici pouze v systémech Kubernetes a Red Hat OpenShift Container Platform. Podporováno podle softwaru IBM MQ .
Funkce: Správci front s více instancemi	K dispozici a podporováno.		K dispozici, ale není podporováno.		K dispozici a podporováno podle softwaru IBM MQ .
Funkce: Typy protokolů pro zotavení	Pouze kruhové protokolování nebo replikované protokoly. Lineární protokolování není podporováno.				K dispozici a podporováno podle softwaru IBM MQ . Musíte nakonfigurovat volby **crtmqm** .
Funkce: určení vlastních voleb příkazového řádku pro crtmqdir, crtmqm, strmqm a endmqm	Není k dispozici a není podporováno. Většinu voleb lze konfigurovat pomocí souboru INI, některé však nelze konfigurovat, například pomocí lineárního protokolování.				Volitelné, v závislosti na způsobu implementace *kódu pro povolení kontejneru*.

	Použití produktu IBM MQ Operator a IBM Cloud Pak for Integration licence	Použití produktu IBM MQ Operator a IBM MQ Advanced licence	Použití produktu IBM MQ Operator a IBM MQ Advanced for Developers licence	Předsestavený IBM MQ Advanced for Developers obraz	Sestavte-svůj-vlastní kontejner
Funkce: Uživatelé operačního systému	Není k dispozici a není podporováno.				Je to možné a podporované podle softwaru IBM MQ , pokud instalujete produkt IBM MQ pomocí RPM, ale není k dispozici žádná ukázka. Nedoporučuje se kvůli bezpečnostním u riziku.
Funkce: IBM MQ Bridge to blockchain	Není k dispozici a není podporováno. Odebráno z produktu IBM MQ zcela od verze IBM MQ 9.3.2 dále.				
Funkce: IBM MQ Bridge to Salesforce	Není k dispozici a není podporováno.				Podporováno na software IBM MQ , ale zamítnuto počínaje produktem IBM MQ 9.3.1 .

Poznámka: Fráze "podporováno podle softwaru IBM MQ " znamená, že technická podpora IBM je omezena na základní software IBM MQ , který je spuštěn v kontejneru.

Související pojmy

Často kladené dotazy k produktu IBM MQ pro vydání Long Term Support a Continuous Delivery

Související odkazy

IBM Cloud Pak for Integration Doplněk životního cyklu softwarové podpory

CP4I-LTS OpenShift CP4I CD Podpora verze pro IBM MQ Operator

Mapování mezi podporovanými verzemi IBM MQ, OpenShift Container Platform a IBM Cloud Pak for Integration.

Poznámka:

IBM MQ Operator podporuje pouze Extended Update Support (EUS) verze OpenShift Container Platform. Informace o tom, která vydání to zahrnuje, naleznete v tématu Fáze životního cyklu na webové stránce Red Hat OpenShift Container Platform Zásada životního cyklu.

- “Dostupné verze produktu IBM MQ” na stránce 12
- “Kompatibilní verze Red Hat OpenShift Container Platform” na stránce 12
- “Verze IBM Cloud Pak for Integration” na stránce 13
- “Dostupné verze produktu IBM MQ ve starších operátorech” na stránce 13
- “Kompatibilní verze OpenShift Container Platform pro starší operátory” na stránce 13

Dostupné verze produktu IBM MQ

Kanál operátoru	Verze operátoru	Verze IBM MQ									
		9.2.0 EUS	9.2.3	9.2.4	9.2.5	9.3.0	9.3.1	9.3.2	9.3.3	9.3.4	9.3.5
v2.0	2.0	→	⚠	●	●	●▯					
v2.1	2.1	→	⚠	⚠	⚠	→	●				
v2.2	2.2	→	⚠	⚠	⚠	→	●				
v2.3	2.3	→	⚠	⚠	⚠	→	⚠	●			
v2.4	2.4	→	⚠	⚠	⚠	→	⚠	⚠	●		
v3.0	3.0					→	⚠	⚠	⚠	●	
v3.1	3.1					→	⚠	⚠	⚠	⚠	●

Klíč:

●
Dostupná podpora Continuous Delivery

▯
IBM Cloud Pak for Integration - Long Term Support k dispozici

→
K dispozici pouze během migrace z operandu IBM Cloud Pak for Integration - Long Term Support na operand Continuous Delivery.

⚠
Deprecated Vzhledem k tomu, že verze produktu IBM MQ přestávají být podporovány, mohou být i nadále konfigurovatelné v operátoru, ale již nejsou způsobilé pro podporu a mohou být odebrány v budoucích verzích.

Úplné podrobnosti o jednotlivých verzích, včetně podrobných funkcí, změn a oprav v jednotlivých verzích viz “Historie vydání pro IBM MQ Operator” na stránce 34.

Kompatibilní verze Red Hat OpenShift Container Platform

Kanál operátoru	Verze operátoru	Verze OpenShift Container Platform[2]		
		4.10	4.12	4.14
v2.0	2.0.0-2.0.15	→	▯	
	2.0.16		▯	
	2.0.17 a dále		▯	▯
v2.1	2.1	→	●	
v2.2	2.2	→	●	
v2.3	2.3	→	●	
v2.4	2.4.0-2.4.3	→	●	
	2.4.4		●	
	2.4.5 a dále		●	●

[2] Verze OpenShift Container Platform jsou předmětem svých vlastních dat podpory. Další informace viz OpenShift Container Platform Life Cycle Policy.

Kanál operátoru	Verze operátoru	Verze OpenShift Container Platform[2]		
		4.10	4.12	4.14
v3.0	3.0.0 a novější		●	●
v3.1	3.1.0 a novější		●	●

Klíč:

●
Dostupná podpora Continuous Delivery

▯
IBM Cloud Pak for Integration - Long Term Support k dispozici

➜
Již není podporováno. Proveďte migraci na novější verzi produktu OpenShift Container Platform .

Verze IBM Cloud Pak for Integration

Podporováno pro použití jako součást produktu IBM Cloud Pak for Integration verze 2022.2.1nebo nezávisle:

- IBM MQ Operator 2.0.x
- IBM MQ Operator 2.1.x

Podporováno pro použití jako součást produktu IBM Cloud Pak for Integration verze 2022.4.1nebo nezávisle:

- IBM MQ Operator 2.2.x
- IBM MQ Operator 2.3.x

Podporováno pro použití jako součást produktu IBM Cloud Pak for Integration verze 2023.2.1nebo nezávisle:

- IBM MQ Operator 2.4.x

Podporováno pro použití jako součást produktu IBM Cloud Pak for Integration verze 2023.4.1nebo nezávisle:

- IBM MQ Operator 3.0.x
- IBM MQ Operator 3.1.x

Dostupné verze produktu IBM MQ ve starších operátorech

Viz Dostupné IBM MQ verze v dokumentaci k produktu IBM MQ 9.2 .

Kompatibilní verze OpenShift Container Platform pro starší operátory

Viz Kompatibilní OpenShift Container Platform verze v dokumentaci k produktu IBM MQ 9.2 .

Plánování licencování IBM MQ v kontejnerech

Licencování kontejnerů vám umožňuje licencovat pouze dostupnou kapacitu jednotlivých kontejnerů IBM MQ , místo abyste museli licencovat celý server, na kterém jsou vaše kontejnery spuštěny. Chcete-li využít výhody licencování kontejnerů, IBM License Service se musí použít ke sledování využití licencí a k určení požadovaného oprávnění.

Související informace

IBM

[2] Verze OpenShift Container Platform jsou předmětem svých vlastních dat podpory. Další informace viz OpenShift Container Platform Life Cycle Policy.

Často kladené dotazy týkající se licencování kontejnerů
Instalace License Service
Zobrazení a sledování využití licencí

Linux Anotace licencí při sestavování vlastního obrazu kontejneru produktu IBM MQ

Anotace licencí umožňují sledovat využití na základě limitů definovaných v kontejneru, a nikoli na základním počítači. Konfigurujete klienty pro implementaci kontejneru se specifickými anotacemi, které IBM License Service používá ke sledování využití.

Při implementaci obrazu vlastního kontejneru produktu IBM MQ se používají dva běžné přístupy k licencování:

- Udělení licence pro celý počítač, na kterém je spuštěn kontejner.
- Udělení licence pro kontejner na základě přiřazených limitů.

Obě volby jsou k dispozici klientům a další podrobnosti lze nalézt na stránce IBM Container Licenses v programu Passport Advantage.

Pokud má být kontejner produktu IBM MQ licencován na základě limitů kontejnerů, je třeba produkt IBM License Service nainstalovat, aby bylo možné sledovat použití. Další informace týkající se podporovaných prostředí a pokynů k instalaci naleznete na stránce ibm-licensing-operator na GitHub.

IBM License Service je nainstalován v klastru Kubernetes, kde je implementován kontejner IBM MQ a kde se ke sledování využití používají anotace Pod. Klienti tedy musejí implementovat Pod se specifickými anotacemi, které pak produkt IBM License Service používá. Na základě vašeho oprávnění a schopností implementovaných v rámci kontejneru použijte jednu nebo více následujících anotací.

Poznámka: Mnoho anotací obsahuje jeden nebo oba následující řádky:

```
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productMetric: "PROCESSOR_VALUE_UNIT" |  "VIRTUAL_PROCESSOR_CORE"
```

Před použitím anotace musíte upravit tyto řádky:

- Pro parametr `productChargedContainers`musíte zvolit `"All"`nebo nahradit skutečný název kontejneru.
- Pro systém `productMetric`musíte zvolit jednu z nabízených hodnot.

Anotace pro použití s nárokem na produkt IBM MQ

Máte-li nárok na produkt IBM MQ , vyberte níže uvedenou anotaci, která odpovídá zakoupenému nároku a kterou chcete použít.

- “IBM MQ” na stránce 16
- “IBM MQ Rozšířené” na stránce 16
- “IBM MQ pro neproduktivní prostředí” na stránce 16
- “IBM MQ Advanced for Non-Production Environment (Rozšířené pro neproduktivní prostředí)” na stránce 17
- “IBM MQ Advanced pro vývojáře” na stránce 17

Anotace IBM MQ , které se mají použít s konfiguracemi vysoké dostupnosti pro více instancí IBM MQ , jsou následující. Další informace najdete v tématu “Výběr správných anotací pro konfigurace vysoké dostupnosti” na stránce 15.

- “IBM MQ Kontejner více instancí” na stránce 17
- “IBM MQ Rozšířené kontejnerové více instancí” na stránce 17
- “IBM MQ Více instancí kontejneru pro neproduktivní prostředí” na stránce 17

- “IBM MQ Advanced Container Multi Instance for Non-Production Environment (Rozšířené více instancí kontejnerů pro neprodukční prostředí)” na stránce 17

Anotace pro použití s oprávněním produktu CP4I

Máte-li nárok na IBM Cloud Pak for Integration (CP4I), vyberte níže uvedenou anotaci, která odpovídá zakoupenému nároku a kterou chcete použít.

- “IBM MQ s CP4I nárokem” na stránce 17
- “IBM MQ Rozšířené s CP4I nárokem” na stránce 18
- “IBM MQ pro neprodukční prostředí s oprávněním CP4I” na stránce 18
- “IBM MQ Rozšířené pro neprodukční prostředí s oprávněním CP4I” na stránce 18

Anotace CP4I , které se mají použít s konfiguracemi vysoké dostupnosti pro více instancí IBM MQ , jsou následující. Další informace najdete v tématu “Výběr správných anotací pro konfigurace vysoké dostupnosti” na stránce 15.

- “IBM MQ Více instancí kontejneru s CP4I nárokem” na stránce 18
- “Oprávnění IBM MQ Advanced Container Multi Instance with CP4I” na stránce 18
- “Oprávnění IBM MQ Container Multi Instance for Non-Production Environment with CP4I” na stránce 18
- “Oprávnění IBM MQ Advanced Container Multi Instance for Non-Production Environment with CP4I” na stránce 19

Výběr správných anotací pro konfigurace vysoké dostupnosti

IBM MQ Více instancí

Při implementaci dvojice správců front v konfiguraci s vysokou dostupností pro více instancí IBM MQ byste měli použít stejnou anotaci v obou instancích. V závislosti na zakoupeném oprávnění by měla být vybrána jedna z následujících anotací:

- IBM MQ nebo IBM MQ Advanced samostatný nárok
  - “IBM MQ Kontejner více instancí” na stránce 17
  - “IBM MQ Rozšířené kontejnerové více instancí” na stránce 17
  - “IBM MQ Více instancí kontejneru pro neprodukční prostředí” na stránce 17
  - “IBM MQ Advanced Container Multi Instance for Non-Production Environment (Rozšířené více instancí kontejnerů pro neprodukční prostředí)” na stránce 17
- IBM Cloud Pak for Integration Nárok
  - “IBM MQ Více instancí kontejneru s CP4I nárokem” na stránce 18
  - “Oprávnění IBM MQ Advanced Container Multi Instance with CP4I” na stránce 18
  - “Oprávnění IBM MQ Container Multi Instance for Non-Production Environment with CP4I” na stránce 18
  - “Oprávnění IBM MQ Advanced Container Multi Instance for Non-Production Environment with CP4I” na stránce 19

Při použití s nárokem IBM Cloud Pak for Integration se poměry nároků v anotacích ujistí, že je zaznamenána správná spotřeba nároku. Při použití se samostatnými nároky IBM MQ nebo IBM MQ Advanced musí být anotace vykázané v License Service pro každou instanci namapovány na části nároku IBM MQ takto:

- IBM MQ Advanced container Více instancí
  - 1 x IBM MQ Advanced **a** 1 x IBM MQ Advanced Replika vysoké dostupnosti **nebo**
  - 2 x IBM MQ Advanced[3]
- IBM MQ Advanced container Více instancí pro neprodukční prostředí

  - 1 x IBM MQ Advanced **a** 1 x IBM MQ Advanced Replika vysoké dostupnosti **nebo**
  - 2 x IBM MQ Advanced pro neprodukční prostředí)[3]
- IBM MQ Kontejner více instancí
  - 1 x IBM MQ **a** 1 x IBM MQ Replika vysoké dostupnosti **nebo**
  - 2 x IBM MQ[3]
- IBM MQ Více instancí kontejneru pro neprodukční prostředí
  - 1 x IBM MQ **a** 1 x IBM MQ Replika vysoké dostupnosti **nebo**
  - 2 x IBM MQ pro neprodukční prostředí) [3]

IBM MQ Nativní HA

Pokud implementujete tři správce front v nativním kvoru vysoké dostupnosti, nárok spotřebovává pouze aktivní instance. Všechny instance by měly mít stejnou anotaci. V závislosti na zakoupeném oprávnění je třeba vybrat jednu z následujících možností:

- IBM MQ nebo IBM MQ Advanced samostatný nárok
  - “IBM MQ Rozšířené” na stránce 16
  - “IBM MQ Advanced for Non-Production Environment (Rozšířené pro neprodukční prostředí)” na stránce 17
- IBM Cloud Pak for Integration Nárok
  - “IBM MQ Rozšířené s CP4I nárokem” na stránce 18
  - “IBM MQ Rozšířené pro neprodukční prostředí s oprávněním CP4I” na stránce 18

Anotace

Zbytek tohoto tématu podrobně popisuje obsah jednotlivých anotací.

IBM MQ

```
productID: "c661609261d5471fb4ff8970a36bccea"
productName: "IBM MQ"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Rozšířené

```
productID: "208423bb063c43288328b1d788745b0c"
productName: "IBM MQ Advanced"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ pro neprodukční prostředí

```
productID: "151bec68564a4a47a14e6fa99266deff"
productName: "IBM MQ for Non-Production Environment"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

[3] Tato volba oprávnění je suboptimální a měla by být použita pouze v případě, že není k dispozici žádný nárok na příslušnou část repliky s vysokou dostupností.

IBM MQ Advanced for Non-Production Environment (Rozšířené pro neproduktivní prostředí)

```
productID: "21dfe9a0f00f444f888756d835334909"
productName: "IBM MQ Advanced for Non-Production Environment"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Advanced pro vývojáře

```
productID: "2f886a3eefbe4ccb89b2adb97c78b9cb"
productName: "IBM MQ Advanced for Developers (Non-Warranted)"
productMetric: "FREE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Kontejner více instancí

```
productID: "2dea73b866b648b6b4abe2a85eb76964"
productName: "IBM MQ Container Multi Instance"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Rozšířené kontejnerové více instancí

```
productID: "bd35bff411bb47c2a3f3a4590f33a8ef"
productName: "IBM MQ Advanced Container Multi Instance"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Více instancí kontejneru pro neproduktivní prostředí

```
productID: "af11b093f16a4a26806013712b860b60"
productName: "IBM MQ Container Multi Instance for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Advanced Container Multi Instance for Non-Production Environment (Rozšířené více instancí kontejnerů pro neproduktivní prostředí)

```
productID: "31f844f7a96b49749130cd0708fdbb17"
productName: "IBM MQ Advanced Container Multi Instance for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ s CP4I nárokem

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "c661609261d5471fb4ff8970a36bccea"
productName: "IBM MQ"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "4:1"
```

IBM MQ Rozšířené s CP4I nárokem

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "208423bb063c43288328b1d788745b0c"
productName: "IBM MQ Advanced"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "2:1"
```

IBM MQ pro neprodukční prostředí s oprávněním CP4I

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "151bec68564a4a47a14e6fa99266deff"
productName: "IBM MQ for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers:  "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "8:1"
```

IBM MQ Rozšířené pro neprodukční prostředí s oprávněním CP4I

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "21dfe9a0f00f444f888756d835334909"
productName: "IBM MQ Advanced for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "4:1"
```

IBM MQ Více instancí kontejneru s CP4I nárokem

```
productName: "IBM MQ Container Multi Instance"
productID: "2dea73b866b648b6b4abe2a85eb76964"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productCloudpakRatio: "10:3"
cloudpakName: "IBM Cloud Pak for Integration"
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
```

Oprávnění IBM MQ Advanced Container Multi Instance with CP4I

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "bd35bff411bb47c2a3f3a4590f33a8ef"
productName: "IBM MQ Advanced Container Multi Instance"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "5:3"
```

Oprávnění IBM MQ Container Multi Instance for Non-Production Environment with CP4I

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "af11b093f16a4a26806013712b860b60"
productName: "IBM MQ Container Multi Instance for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "20:3"
```

Oprávnění IBM MQ Advanced Container Multi Instance for Non-Production Environment with CP4I

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "31f844f7a96b49749130cd0708fdbb17"
productName: "IBM MQ Advanced Container Multi Instance for Non-Production Environments"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "10:3"
```

OpenShift CP4I Závislosti pro IBM MQ Operator

Od verze IBM MQ Operator 3.0 se při instalaci produktu IBM MQ Operatorautomaticky nenainstalují žádné další operátory. Ve starších verzích produktu IBM MQ Operatorexistuje tvrdá závislost na produktu IBM Cloud Pak foundational services , který také instaluje operátor IBM Operand Deployment Lifecycle Manager (ODLM).

Operátor licencování IBM musí být nainstalován odděleně, aby bylo možné sledovat využití licencí. Viz Implementace License Service v dokumentaci k produktu IBM Cloud Pak for Integration .

IBM MQ Operator 3.0 a novější

V 9.3.4

Když vytvoříte `QueueManager` pomocí licence na produkt IBM Cloud Pak for Integration , můžete zvolit, zda chcete použít jednotné přihlášení s instancí IBM Cloud Pak for Integration Keycloak. Použití Keycloak je standardně povoleno s licencí IBM Cloud Pak for Integration , ale pokud není nainstalováno, produkt `QueueManager` přejde do stavu "Blokováno", dokud nebudou nainstalovány správné závislosti. Další podrobnosti o závislostech viz “Instalace produktu IBM MQ Operator” na stránce 101 .

Starší verze produktu IBM MQ Operator

Operátory IBM Cloud Pak foundational services se nainstalují automaticky, když nainstalujete starší verze produktu the IBM MQ Operator. Tito závislí operátoři mají malý prostor CPU a paměťový nárok a používají se k implementaci dalších prostředků za určitých okolností.

Když vytváříte `QueueManager`, IBM MQ Operator vytvoří operand `OperandRequest` pro další služby, které potřebuje. Agent `OperandRequest` je splněn operátorem ODLM a v případě potřeby nainstaluje a vytvoří instanci požadovaných služeb. Které služby jsou vyžadovány, je určeno na základě licenční smlouvy přijaté při implementaci správce front a na základě kterých komponent správce front jsou požadovány.

- Vyberete-li licenci IBM MQ Advanced nebo IBM MQ Advanced for Developers, nebudou vyžadovány žádné další služby. Například v následujícím případě se IBM Cloud Pak foundational services nepoužívá:

  ```
  spec:
    license:
      accept: true
      license: L-AMRD-XH6P3Q
      use: "Production"
  ```

- Pokud vyberete licenci IBM Cloud Pak for Integration a vyberete povolení webového serveru, IBM MQ Operator také vytvoří instanci operátoru IBM Identity and Access Management (IAM), aby povolil jednotné přihlášení. Operátor IAM bude vždy k dispozici, pokud jste nainstalovali operátor IBM Cloud Pak for Integration. Příklad:

  ```
  spec:
    license:
      accept: true
      license: L-RJON-CD3JKX
      use: "Production"
  ```

Pokud však zakážete webový server, nevyžaduje se IBM Cloud Pak foundational services. Příklad:

```
spec:
  license:
    accept: true
    license: L-RJON-CD3JKX
    use: "Production"
  web:
    enabled: false
```

Podrobný rozpis požadavků na hardware a software pro závislé operátory viz Požadavky na hardware a doporučení pro základní služby.

Můžete si vybrat množství CPU a paměti, které vaši správci front používají. Další informace naleznete v tématu “.spec.queueManager.resources” na stránce 188.

Související odkazy

“Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 179

OpenShift CP4I Oprávnění s vymezeným klastrem vyžadovaná produktem IBM MQ Operator

Produkt IBM MQ Operator vyžaduje oprávnění s vymezeným klastrem ke správě webhooků pro příjem a ukázek a ke čtení informací o třídě úložiště a verzi klastru.

IBM MQ Operator vyžaduje následující oprávnění s vymezeným klastrem:

- Oprávnění ke správě webhooků pro příjem. To umožňuje vytvářet, načítat a aktualizovat specifické webhooky, které se používají v procesu vytváření a správy kontejnerů poskytnutých operátorem.
  - Skupiny rozhraní API: **admissionregistration.k8s.io**
  - Prostředky: **validatingwebhookconfigurations**
  - Slovesa: **get, delete**
- Oprávnění k vytváření a správě prostředků, které se používají v konzole Red Hat OpenShift k poskytování ukázek a úseků kódu při vytváření vlastních prostředků.
  - Skupiny rozhraní API: **console.openshift.io**
  - Prostředky: **consoleyamlsamples**
  - Slovesa: **create, get, update, delete**
- Oprávnění ke čtení verze klastru. Operator tak může vrátit zpět veškeré problémy s prostředím klastru.
  - Skupiny rozhraní API: **config.openshift.io**
  - Prostředky: **clusterversions**
  - Slovesa: **get, list, watch**
- Oprávnění ke čtení paměťových tříd v klastru. Operator tak může vrátit zpět veškeré problémy s vybranými paměťovými třídami úložiště v kontejnerech.
  - Skupiny rozhraní API: **storage.k8s.io**
  - Prostředky: **storageclasses**
  - Slovesa: **get, list**

Poznámka: Produkt IBM MQ Operator také vyžaduje oprávnění v rozsahu oboru názvů. Pokud je agent IBM MQ Operator nainstalován v rozsahu klastru, pak jsou oprávnění v rozsahu oboru názvů přítomna ve všech oborech názvů.

OpenShift CP4I Kubernetes Aspekty úložiště pro IBM MQ Operator

IBM MQ Operator se spouští ve dvou režimech úložiště:

- **Přechodné úložiště** se používá, když se všechny stavové informace pro kontejner mohou vyřadit po restartu kontejneru. 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 Operator 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 používáte dočasné úložiště, všechny informace o stavu správce front se při restartu ztratí. To zahrnuje:

- Všechny zprávy.
- Všichni správci front do stavu komunikace správce front (pořadová čísla zpráv kanálu).
- Identita 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 pomocí vlastních souborů MQSC a INI s použitím rozhraní CLI Red Hat OpenShift” na stránce 162). Není-li tento proces dokončen, bude muset být při každém restartování kontejneru nakonfigurován produkt IBM MQ.

OpenShift CP4I Chcete-li např. nakonfigurovat produkt IBM MQ s přechodným úložištěm, měl by typ úložiště `QueueManager` obsahovat následující:

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

Trvalé úložiště

OpenShift CP4I

Produkt IBM MQ se obvykle spouští s trvalým úložištěm, aby se zajistilo, že správce front uchová své trvalé zprávy a konfiguraci po restartu. Toto chování je výchozí. Vzhledem k tomu, že existují různí poskytovatelé úložišť, z nichž každý podporuje různé schopnosti, často to znamená, že je vyžadováno přizpůsobení konfigurace. Níže uvedený příklad uvádí obecná pole, která upravují konfiguraci úložiště IBM MQ v rozhraní API v1beta1 :

- **`spec.queueManager.availability`** řídí režim dostupnosti. Pokud používáte `SingleInstance` nebo `NativeHA`, potřebujete pouze úložiště `ReadWriteOnce` . Pro systém `multiInstance` požadujete paměťovou třídu, která podporuje `ReadWriteMany` se správnou charakteristikou 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 v kontejnerech” na stránce 25.
- **`spec.queueManager.storage`** řídí individuální nastavení úložiště. Správce front lze konfigurovat pro použití mezi jedním a čtyřmi trvalými 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:
        class: ibmc-file-gold-gid
      persistedData:
        enabled: true
        class: ibmc-file-gold-gid
      recoveryLogs:
        enabled: true
        class: ibmc-file-gold-gid
  securityContext:
     supplementalGroups: [65534] # Change to 99 for clusters with RHEL7 or earlier worker nodes
```

Informace o aspektech úložiště pro správce front nativní vysoké dostupnosti naleznete v tématu “Nativní vysoká dostupnost” na stránce 141.

Poznámka: Doplňkové skupiny můžete také konfigurovat pomocí správců front s jednou instancí.

Kapacita úložiště

OpenShift CP4I

Při použití konzoly IBM MQ Operatorje požadovaná velikost úložiště pevná a nelze ji po vytvoření správce front změnit. Musíte se ujistit, že je svazek dostatečně velký pro vaše potřeby.

Šifrování

OpenShift CP4I

IBM MQ aktivně nešifruje data v klidu. Proto byste měli k šifrování zpráv použít pasivně šifrované úložiště, IBM MQ Advanced Message Securitynebo obojí. V systému IBM Cloud je k dispozici úložiště bloků i souborů s pasivním šifrováním v klidu.

OpenShift CP4I Kubernetes IBM MQ Advanced for Developers obrázek kontejneru

Předem sestavený obraz kontejneru je k dispozici pro IBM MQ Advanced for Developers. Tento obrázek je k dispozici v adresáři IBM Container Registry. Tento obraz je vhodný pro použití s Docker, Podman, Kubernetesa dalšími kontejnerovými prostředími.

Poznámka: Deprecated Obrazy produktu IBM MQ Advanced for Developers byly dříve dostupné z centrálního serveru Docker , ale toto je zamítnuto a na centrálním serveru Docker nejsou k dispozici žádné další aktualizace.

Dostupné obrázky

Obrazy IBM MQ jsou uloženy v adresáři IBM Container Registry:

- IBM MQ Advanced for Developers 9.3.0.17: `icr.io/ibm-messaging/mq:9.3.0.17-r3`
- IBM MQ Advanced for Developers 9.3.5.1: `icr.io/ibm-messaging/mq:9.3.5.1-r2`

Rychlá reference

- license:
  - IBM MQ Advanced for Developers a Apache Licence 2.0. Všimněte si, že licence na produkt IBM MQ Advanced for Developers nepovoluje další distribuci a podmínky omezují použití na počítač vývojáře.
- Kam se mají uložit problémy:
  - GitHub
- K dispozici pro následující architektury CPU:
  - amd64
  - s390x
  - ppc64le

Pouľití

Spusťte IBM MQ Advanced for Developers v kontejneru.

Podrobnosti o tom, jak spustit kontejner, naleznete v dokumentaci k použití .

Chcete-li používat obraz, musíte přijmout podmínky licence na produkt IBM MQ nastavením proměnné prostředí **LICENSE** .

Podporované proměnné prostředí

LANG
Nastavte jazyk, ve kterém chcete licenci vytisknout.

Licence
Nastavte volbu `accept` tak, aby souhlasila s licenčními podmínkami IBM MQ Advanced for Developers .

Nastavte `zobrazení` , chcete-li zobrazit podmínky licence.

Deprecated **LOG_FORMAT**
ZAMÍTNUTO: nahrazeno pomocí “[MQ 9.3.2 Feb 2023]MQ_LOGGING_CONSOLE_FORMAT” na stránce 24.

Změňte formát protokolů, které se vytisknou do umístění `stdout` kontejneru.

Nastavte volbu `basic` tak, aby používala jednoduchý formát čitelný pro člověka. Toto je výchozí hodnota.

Nastavte `json` pro použití formátu JSON (jeden objekt JSON na každém řádku).

Deprecated **MQ_ADMIN_PASSWORD**
Zadejte heslo administrativního uživatele.

Musí mít alespoň 8 znaků.

V 9.3.4 Pro uživatele s oprávněním administrátora neexistuje žádné výchozí heslo. Pro verze systému IBM MQ Operator starší než 3.0.0je výchozí hodnota `passw0rd`.

V 9.3.4 V systému IBM MQ 9.3.4je tato proměnná zamítnuta. Příklad YAML v tomto tématu ukazuje, jak můžete vytvořit tuto proměnnou sami a zabezpečit ji tajným klíčem.

Deprecated **MQ_APP_PASSWORD**
Zadejte heslo uživatele aplikace.

Je-li nastaveno, způsobí, že kanál **DEV.APP.SVRCONN** bude zabezpečen a povolí pouze připojení, která dodávají platné ID uživatele a heslo.

Musí mít alespoň 8 znaků.

V 9.3.4 Pro uživatele aplikace neexistuje žádné výchozí heslo. Pro verze produktu IBM MQ Operator starší než 3.0.0je výchozí hodnota prázdná (není vyžadováno heslo) pro klienty IBM MQ a `passw0rd` pro klienty HTTP.

V 9.3.4 V systému IBM MQ 9.3.4je tato proměnná zamítnuta. Příklad YAML v tomto tématu ukazuje, jak můžete vytvořit tuto proměnnou sami a zabezpečit ji tajným klíčem.

MQ_DEV
Nastavte hodnotu `false` , chcete-li zastavit vytvářené výchozí objekty.

MQ_ENABLE_METRICS
Nastavte hodnotu `true` , chcete-li generovat metriky Prometheus pro vašeho správce front.

V 9.3.2 **MQ_LOGGING_CONSOLE_SOURCE**
Zadejte čárkami oddělený seznam zdrojů pro protokoly, které jsou zrcadleny do umístění **stdout** kontejneru.

Platné hodnoty jsou `qmgr` a `web`.

Výchozí hodnota je `qmgr, web`.

V 9.3.2 **MQ_LOGGING_CONSOLE_FORMAT**
Nahrazuje “[Zamítnuto]LOG_FORMAT” na stránce 23.

Změňte formát protokolů, které se vytisknou do umístění **stdout** kontejneru.

Nastavte volbu `basic` tak, aby používala jednoduchý formát čitelný pro člověka. Toto je výchozí hodnota.

Nastavte `json` pro použití formátu JSON (jeden objekt JSON na každém řádku).

V 9.3.2 **MQ_LOGGING_CONSOLE_EXCLUDE_ID**
Zadejte seznam ID zpráv oddělených čárkami pro zprávy protokolu, které jsou vyloučeny.

Zprávy protokolu se stále objevují v souboru protokolu na disku, ale nejsou vytištěny do umístění **stdout** kontejneru.

Výchozí hodnota je `AMQ5041I,AMQ5052I,AMQ5051I,AMQ5037I,AMQ5975I`.

MQ_QMGR_NAME
Nastavte název, se kterým má být vytvořen váš správce front.

Další informace o výchozí konfiguraci vývojáře podporované obrazem IBM MQ Advanced for Developers naleznete v dokumentaci k výchozí konfiguraci vývojáře.

V 9.3.4 Příklad správce front YAML, který popisuje, jak zadat hesla pro admin a app uživatele

Od verze IBM MQ 9.3.4již ID uživatelů **admin** a **app** nemají výchozí hesla. Pro tyto uživatele musíte zadat hesla při implementaci správce front pomocí licence na produkt `Development` . Zde je příklad správce front YAML, který ukazuje, jak to provést s IBM MQ Operator.

Následující příkaz vytvoří tajný klíč obsahující hesla pro uživatele **admin** a **app** .

```
oc create secret generic my-mq-dev-passwords --from-literal=dev-admin-password=passw0rd --from-
literal=dev-app-password=passw0rd
```

Následující YAML používá tato hesla při implementaci správce front.

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm-dev
spec:
  license:
    accept: false
    license: L-AXAF-JLZ53A
    use: Development
  web:
```

```
    enabled: true
  template:
    pod:
      containers:
        - env:
            - name: MQ_DEV
              value: "true"
            - name: MQ_CONNAUTH_USE_HTP
              value: "true"
            - name: MQ_ADMIN_PASSWORD
              valueFrom:
                secretKeyRef:
                  name: my-mq-dev-passwords
                  key: dev-admin-password
            - name: MQ_APP_PASSWORD
              valueFrom:
                secretKeyRef:
                  name: my-mq-dev-passwords
                  key: dev-app-password
          name: qmgr
  queueManager:
    storage:
      queueManager:
        type: persistent-claim
    name: QUICKSTART
  version: 9.3.5.1-r2
```

OpenShift CP4I Kubernetes Vysoká dostupnost pro IBM MQ v kontejnerech

Existují tři volby pro vysokou dostupnost s produktem IBM MQ Operator: **Nativní správce front HA** (který má aktivní repliku a dvě záložní repliky), **Správce front s více instancemi** (což je dvojice aktivní-pohotovostní, používající sdílený, síťový systém souborů) nebo **Jeden správce front schopný obnovy** (který nabízí jednoduchý přístup pro vysokou dostupnost pomocí síťového úložiště). Druhá z těchto dvou možností závisí na systému souborů, aby se zajistila dostupnost obnovitelných dat, ale nativní vysoká dostupnost nikoli. Proto, když nepoužíváte Nativní vysokou dostupnost, je dostupnost systému souborů kritická pro dostupnost správce front. Tam, kde je obnova dat důležitá, by měl systém souborů zajistit redundanci pomocí replikace.

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 nativní vysoké dostupnosti

CP4I MQ Adv.

Nativní správci front HA zahrnují **aktivní** a dvě **repliky** Kubernetes pody, které jsou spuštěny jako součást Kubernetes StatefulSet s přesně třemi replikami, z nichž každá má svou vlastní sadu Kubernetes trvalých svazků. Požadavky na IBM MQ pro sdílené systémy souborů také platí pro použití správce front nativní vysoké dostupnosti (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 správce front nativní vysoké dostupnosti jsou řízeny následujícími faktory:

1. Jak dlouho trvá instancím repliky zjistit, že aktivní instance se nezdařila. Toto je konfigurovatelné.

2. Jak dlouho trvá sondě připravenost podu Kubernetes zjistit, že je kontejner připraven se změnit a přesměrovat síťový provoz. Toto je konfigurovatelné.
3. Jak dlouho trvá, než se klienti IBM MQ znovu připojí.

Další informace viz téma “Nativní vysoká dostupnost” na stránce 141.

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 připravenost podu Kubernetes zjistit, že je kontejner připraven se změnit a přesměrovat síťový provoz. Toto je konfigurovatelné.
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 je konfigurovatelné.
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 je konfigurovatelné.
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 při použití stavové pracovní zátěže, jako je IBM MQ s Kubernetes StatefulSet, ztratí hlavní uzel systému Kubernetes kontakt s pracovním uzlem, nemůže určit, zda došlo k selhání uzlu nebo zda došlo 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.

Poznámka: Změna podrobností StatefulSet správce front IBM MQ , včetně počtu replik, není při vytváření správce front prostřednictvím konzoly IBM MQ Operatorpodporována.

Související pojmy

Konfigurace vysoké dostupnosti

Související úlohy

“Konfigurace vysoké dostupnosti pro správce front pomocí IBM MQ Operator” na stránce 141

OpenShift CP4I Kubernetes Zotavení z havárie pro produkt IBM MQ v kontejnerech

Musíte zvážit, na jakou havárii se chystáte. V prostředích cloudu poskytují zóny dostupnosti určitou úroveň tolerance k haváriím, a používání je mnohem snazší. Pokud máte lichý počet datových středisek (pro kvorum) a síťový odkaz s nízkou latencí, mohli byste potenciálně spustit jeden klastr Red Hat OpenShift Container Platform nebo Kubernetes s více zónami dostupnosti, každý v odděleném fyzickém umístění. Toto téma probírá aspekty pro zotavení z havárie, kde nelze splnit tato kritéria: to znamená buď sudý počet datových středisek, nebo síťový odkaz s vysokou latencí.

Pro zotavení z havárie je třeba vzít v úvahu následující skutečnosti:

- Replikace dat produktu IBM MQ (držených v jednom nebo více prostředcích `PersistentVolume`) do umístění pro zotavení z havárie
- Opětovné vytvoření správce front s použitím replikovaných dat.
- ID sítě správce front, které je viditelné pro aplikace klienta produktu IBM MQ a další správce front. Toto ID může být např. položkou DNS.

Trvalá data je třeba replikovat, buď synchronně, nebo asynchronně na server pro zotavení z havárie. Tento stav je obvykle specifický pro poskytovatele úložiště, ale lze jej také provést pomocí produktu `VolumeSnapshot`. Další informace o snímcích svazku viz Snímky svazku CSI.

Při zotavování z havárie budete muset znovu vytvořit instanci správce front na novém klastru Kybernetes s použitím replikovaných dat. Pokud používáte produkt IBM MQ Operator, budete potřebovat YAML produktu `QueueManager`, stejně jako YAML pro další podpůrné prostředky, jako například `ConfigMap` nebo `Secret`.

Související informace

ha_for_ctr.dita

OpenShift CP4I Plánování zabezpečení produktu IBM MQ v kontejnerech

Aspekty zabezpečení při plánování produktu IBM MQ v konfiguraci kontejnerů.

Procedura

- “Ověření uživatele a autorizace pro produkt IBM MQ v kontejnerech” na stránce 28
  - “Bezpečnostní omezení pro použití uživatelů operačního systému v kontejnerech” na stránce 28
- “Aspekty omezení síťového přenosu na IBM MQ v kontejnerech” na stránce 29

Ověření uživatele a autorizace pro produkt IBM MQ v kontejnerech

Produkt IBM MQ v kontejnerech lze konfigurovat tak, aby ověřoval uživatele prostřednictvím protokolu LDAP, vzájemného TLS nebo vlastního modulu plug-in produktu MQ .

Všimněte si, že operátor IBM MQ nepovoluje použití uživatelů a skupin operačního systému v rámci obrazu kontejneru. Další informace viz téma “Bezpečnostní omezení pro použití uživatelů operačního systému v kontejnerech” na stránce 28.

LDAP

Informace o konfiguraci produktu IBM MQ pro použití úložiště uživatelů LDAP naleznete v tématu Ověřování připojení: Úložiště uživatelů a Autorizace LDAP.

Vzájemný protokol TLS

Pokud konfigurujete příchozí připojení ke správci front tak, aby vyžadovala certifikát TLS (vzájemné TLS), můžete namapovat rozlišující název certifikátu na jméno uživatele. Musíte udělat dvě věci:

- Nakonfigurujte záznam ověřování kanálu pro vytvoření mapování na jméno uživatele pomocí SSLPEER. Další informace naleznete v tématu Mapování rozlišujícího názvu SSL nebo TLS na ID uživatele MCAUSER.
- Nakonfigurujte správce front tak, aby vám umožňoval definovat záznamy oprávnění pro jméno uživatele, které systém nezná. Další informace viz Sekce služby souboru qm.ini.

Webové tokeny JSON

Informace o konfiguraci produktu IBM MQ pro použití webových tokenů JSON (JWT) viz Práce s tokeny ověření.

Vlastní modul plug-in produktu MQ

Jedná se o pokročilou techniku a vyžaduje mnohem více práce. Další informace naleznete v tématu Použití vlastní autorizační služby.

Související úlohy

“Příklad: Konfigurace správce front s vzájemným ověřením TLS” na stránce 136
Tento příklad implementuje správce front do produktu OpenShift Container Platform pomocí IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

Bezpečnostní omezení pro použití uživatelů operačního systému v kontejnerech

Použití uživatelů operačního systému v kontejnerech se nedoporučuje a je u operátora IBM MQ zakázáno.

V kontejnerizovaném prostředí s více nájemci jsou obvykle k dispozici omezení zabezpečení, aby se zabránilo možným problémům se zabezpečením, například:

- **Zabránění použití uživatele "root" uvnitř kontejneru.**
- **Vynucení použití náhodného UID**. Například v Red Hat OpenShift Container Platform používá pro každý kontejner výchozí `SecurityContextConstraints` (s názvem `restricted`) náhodné ID uživatele.
- **Zabránění použití eskalace oprávnění**. IBM MQ on Linux používá eskalaci oprávnění ke kontrole hesel uživatelů-používá program "setuid", aby se stal uživatelem "root".

OpenShift CP4I Pro zajištění shody s těmito bezpečnostními opatřeními produkt IBM MQ Operator nepovoluje použití ID, která jsou definována v knihovnách operačního systému v kontejneru. V kontejneru není definováno žádné ID uživatele nebo skupiny `mqm`.

Aspekty omezení síťového přenosu na IBM MQ v kontejnerech

V produktu OpenShift Container Platform a Kubernetesmůžete nadefinovat zásady sítě, které omezí provoz na sekce ve vašem klastru. Toto téma popisuje některé aspekty týkající se toho, jak mohou zásady sítě platit pro produkt IBM MQ.

V případě síťové kolekce pravidel Ingress pro správce front je třeba zvážit několik portů:

- Port 1414 pro provoz správce front
- Port 9414 pro nativní vysokou dostupnost
- Port 9157 pro metriky
- Port 9443 pro webovou konzolu a rozhraní REST API

Výstup ze sítě je složitější. Příklady výstupu do sítě, které byste mohli zvážit:

- DNS-pokud máte kanály nebo jinou konfiguraci, která používá názvy DNS
- Další správci front
- Protokol OCSP (Online Certificate Status Protocol) a seznamy odvolaných certifikátů (CRL)-určuje váš poskytovatel certifikátů.
- Poskytovatelé ověření:
  - LDAP
  - Otevřete ID Connect nebo jiného nakonfigurovaného poskytovatele přihlášení pro webový server IBM MQ . To zahrnuje uživatelské rozhraní IBM Cloud Pak Platform UI a základní služby IBM Cloud Pak IAM.
- Poskytovatelé trasování:
  - Vytvořit instanci
  - Řídicí panel operací Cloud Pak for Integration[4]

Příklad ingress NetworkPolicy

Následuje příklad zásady sítě pro řízení kolekce pravidel Ingress pro správce front s názvem "myqm" pro použití na platformě Red Hat OpenShift Container Platform.

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

[4] Řídicí panel operací byl zamítnut z produktu IBM MQ 9.3.0a odebrán z adresáře IBM MQ 9.3.3. Viz téma “Integrace s IBM Cloud Pak for Integration Operations Dashboard” na stránce 154.

```
    ports:
      - protocol: TCP
        port: 9157
  # Allow access to web server via Route
  - from:
      - namespaceSelector:
          matchLabels:
            network.openshift.io/policy-group: ingress
    ports:
      - protocol: TCP
        port: 9443
```

Shoda s FIPS pro IBM MQ v kontejnerech

Při spuštění produkt IBM MQ v kontejnerech zjistí, zda operační systém, na kterém se kontejner spouští, vyhovuje standardu FIPS, a (pokud ano) automaticky nakonfiguruje podporu FIPS. Zde jsou uvedeny požadavky a omezení.

Federální standardy zpracování informací

Americká vláda poskytuje technické poradenství v oblasti IT systémů a bezpečnosti, včetně šifrování dat. National Institute for Standards and Technology (NIST) je vládní orgán zabývající se IT systémy a bezpečností. NIST vytváří doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

Významným standardem FIPS je standard FIPS 140-2, který vyžaduje použití silného šifrovacího algoritmu. Standard FIPS 140-2 také uvádí požadavky na hašovací algoritmy, které se mají použít k ochraně paketů před úpravami při přenosu.

Produkt IBM MQ poskytuje podporu FIPS 140-2, pokud k tomu byl nakonfigurován.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Požadavky

Další informace o požadavcích souvisejících s nastavením klastru a dalších aspektech naleznete v tématu FIPS Wall: Aktuální IBM přístup ke shodě se standardem FIPS.

Produkt IBM MQ v kontejnerech může být spuštěn v režimu shody FIPS 140-2. Během spuštění produkt IBM MQ v kontejnerech (9.3.1.0 a vyšší) zjistí, zda operační systém hostitele, na kterém se kontejner spouští, vyhovuje standardu FIPS. Pokud je hostitelský operační systém kompatibilní se standardem FIPS a byly dodány soukromé klíče a certifikáty, kontejner IBM MQ nakonfiguruje správce front, webový server IBM MQ a přenos dat mezi uzly v implementaci nativní vysoké dostupnosti pro spuštění v režimu shody se standardem FIPS.

Při použití produktu IBM MQ Operator k implementaci správců front operátor vytvoří trasu s typem ukončení **Passthrough**. To znamená, že provoz je odeslán přímo do místa určení, aniž by směrovač poskytoval ukončení TLS. Správce front IBM MQ a webový server IBM MQ jsou v tomto případě cíli a již poskytují zabezpečenou komunikaci v souladu se standardem FIPS.

Klíčové požadavky:

1. Soukromý klíč a certifikáty poskytnuté v tajném údaji správci front a webovému serveru, které umožňují externím klientům zabezpečené připojení ke správci front a webovému serveru.
2. Soukromý klíč a certifikáty pro přenos dat mezi různými uzly v konfiguraci nativní vysoké dostupnosti.

Omezení

Pro implementaci produktu IBM MQ v kontejnerech vyhovující standardu FIPS zvažte následující:

- IBM MQ v kontejnerech poskytuje koncový bod pro kolekci metrik. Momentálně je tento koncový bod pouze HTTP. Koncový bod metrik můžete vypnout, aby byl zbytek standardu IBM MQ FIPS kompatibilní.
- IBM MQ v kontejnerech umožňuje vlastní přepsání obrázku. To znamená, že můžete sestavit vlastní obrazy pomocí obrazu kontejneru IBM MQ jako základního obrazu. Pro tyto upravené obrazy nemusí být použita shoda se standardem FIPS.
- Pro sledování zpráv pomocí produktu IBM Instanaje komunikace mezi IBM MQ a IBM Instana HTTP nebo HTTPS, bez shody se standardem FIPS.
- IBM MQ Operator access to IBM identity and access management (IAM) /Zen services není kompatibilní se standardem FIPS.

Způsob zjištění shody se standardem FIPS a automatická konfigurace podpory FIPS

Pokud operační systém, na kterém se kontejner spouští, vyhovuje standardu FIPS, podpora FIPS se nakonfiguruje automaticky.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Během spouštění produkt IBM MQ v kontejnerech zjistí, zda operační systém, na kterém se kontejner spouští, vyhovuje standardu FIPS. Pokud ano, jsou automaticky provedeny následující akce:

Správce front
Pokud operační systém hostitele vyhovuje standardu FIPS a je dodán soukromý klíč a certifikáty, atribut správce front **SSLFIPS** je nastaven na hodnotu YES. Jinak je atribut **SSLFIPS** nastaven na hodnotu NO.

IBM MQ webový server
Webový server IBM MQ poskytuje rozhraní HTTP/HTTPS pro administraci IBM MQ. Pokud operační systém hostitele vyhovuje standardu FIPS, volby prostředí JVM se aktualizují, aby webový server používal šifrování vyhovující standardu FIPS. Chcete-li používat standard FIPS, musí být soukromý klíč a certifikáty dodány během spuštění kontejneru.

Nativní vysoká dostupnost
Zabezpečení dat replikovaných mezi uzly je řízeno sekcí **NativeHALocalInstance** souboru `qm.ini` . Příklad:

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

Je-li povolen standard FIPS, atribut **SSLFipsRequired** se přidá do sekce s hodnotou nastavenou na Ano:

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

Pokud je kontejner spuštěn v klastru OpenShift bez podpory FIPS, pak správce front, webový server IBM MQ a nativní komponenty HA nemají automaticky povolenou podporu FIPS. Pouze architektura x86-64 je momentálně podporována platformou OpenShift pro FIPS. V případě architektur Power a Linux for IBM Z produkt OpenShift nenabízí podporu FIPS. Chcete-li explicitně povolit podporu FIPS v komponentách IBM MQ pro tyto architektury, nastavte proměnnou prostředí *MQ_ENABLE_FIPS* ve správci front YAML na hodnotu `true` . Následující úsek YAML popisuje použití proměnné prostředí *MQ_ENABLE_FIPS* :

```
template:
    pod:
      containers:
        - env:
            - name: MQ_ENABLE_FIPS
```

```
            value: "true"
          name: qmgr
```

Potlačení automatického režimu FIPS pro IBM MQ v kontejnerech

Pomocí proměnné prostředí *MQ_ENABLE_FIPS* explicitně povolíte nebo zakážete režim FIPS pro komponenty IBM MQ v kontejneru.

Než začnete

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Informace o této úloze

MQ_ENABLE_FIPS podporuje tři hodnoty:

automaticky
Toto je výchozí hodnota.

Pokud je v hostitelském operačním systému povolen standard FIPS, všechny komponenty (správce front, webový server IBM MQ a nativní vysoká dostupnost) se spustí v režimu FIPS.

Pokud operační systém hostitele není povolen FIPS, pak se všechny komponenty nespustí v režimu FIPS.

ano
Tato hodnota zapíná standard FIPS pro vybrané komponenty v kontejneru.

Atribut správce front **SSLFIPS** je nastaven na hodnotu YES , i když IBM MQ v kontejnerech běží na hostitelském operačním systému, který nevyhovuje standardu FIPS. To znamená, že pokud správce front IBM MQ , webový server a nativní vysoká dostupnost vyhovují standardu FIPS, operační systém kontejneru tomu tak není.

ne
Tato hodnota vypne kompatibilitu se standardem FIPS.

Atribut správce front **SSLFIPS** je nastaven na hodnotu NO, a to i v případě, že je produkt IBM MQ v kontejnerech spuštěn na hostitelském počítači kompatibilním se standardem FIPS. Produkt IBM MQ však stále zabezpečuje připojení, pokud jsou dodány soukromý klíč a certifikáty.

Volby prostředí JVM nejsou aktualizovány pro webový server IBM MQ . Webový server IBM MQ však stále spouští koncový bod HTTPS, pokud je dodán soukromý klíč a certifikáty.

Replikace dat v nativní vysoké dostupnosti nepoužívá šifrování FIPS.

Příklad

Zde je ukázkový správce front YAML, který popisuje povolení TLS a FIPS pro komponentu správce front:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  namespace: ibm-mq-fips
  name: ibm-mq-qm-ppcle
spec:
  license:
    accept: true
    license: L-AMRD-XH6P3Q
    use: Production
  queueManager:
    name: PPCLEQM
    storage:
      queueManager:
        type: ephemeral
  template:
    pod:
```

```
    containers:
      - env:
          - name: MQ_ENABLE_FIPS
            value: "true"
        name: qmgr
version: 9.3.5.1-r2
web:
  enabled: false
pki:
  keys:
    - name: ibm-mq-tls-certs
      secret:
        secretName: ibm-mq-tls-secret
        items:
        - tls.key
        - tls.crt
```

Multi Plánování rozšiřitelnosti a výkonu pro produkt IBM MQ v kontejnerech

Ve většině případů je škálování a výkon produktu IBM MQ v kontejnerech stejný jako u produktu IBM MQ for Multiplatforms. Existuje však několik dalších limitů, které mohou být stanoveny kontejnerovou platformou.

Informace o této úloze

Při plánování rozšiřitelnosti a výkonu pro produkt IBM MQ v kontejnerech zvažte následující volby:

Procedura

- **Omezit počet podprocesů a procesů.**

  Produkt IBM MQ používá podprocesy ke správě souběžnosti. V produktu Linuxjsou podprocesy implementovány jako procesy, takže můžete narazit na limity stanovené platformou kontejneru nebo operačním systémem na maximální počet procesů. V produktu Red Hat OpenShift Container Platform 4.11existuje výchozí limit 4096 procesů na kontejner. Pro starší verze produktu OpenShift Container Platform je limit 1024 procesů. Kompatibilitu verzí produktu IBM MQ Operator s verzemi produktu OpenShift Container Platform viz “Kompatibilní verze Red Hat OpenShift Container Platform” na stránce 12. I když je to adekvátní pro většinu scénářů, mohou nastat případy, kdy to může mít vliv na počet připojení klienta pro správce front.

  Limit procesů v produktu Kubernetes může konfigurovat administrátor klastru pomocí nastavení konfigurace kubelet **podPidsLimit**. Viz Omezení ID procesu a rezervace v dokumentaci k produktu Kubernetes . V produktu Red Hat OpenShift Container Platformmůžete také vytvořit **ContainerRuntimeConfig** vlastní prostředek pro úpravu parametrů CRI-O.

  V konfiguraci produktu IBM MQ můžete také nastavit maximální počet připojení klienta pro správce front. Informace o použití omezení pro jednotlivé kanály připojení serveru naleznete v tématu Omezení pro kanály připojení serveru a o použití omezení pro celého správce front v části MAXCHANNELS INI .

- **Omezit počet svazků.**

  V cloudových a kontejnerových systémech se běžně používají svazky úložišť připojené k síti. Existují omezení počtu svazků, které lze připojit k uzlům Linux . Například AWS EC2 omezuje na maximálně 30 svazků na jeden virtuální počítač. Red Hat OpenShift Container Platform má podobný limit, stejně jako Microsoft Azure a Google Cloud Platform.

  Nativní správce front HA vyžaduje jeden svazek pro každou ze tří instancí a vynucuje rozložení instancí mezi uzly. Správce front však můžete nakonfigurovat tak, aby používal tři svazky pro každou instanci (data správce front, protokoly pro zotavení a trvalá data).

- **Použijte IBM MQ techniky škálování.**

  Namísto malého počtu velkých správců front může být výhodné použít IBM MQ metody škálování, jako např. IBM MQ uniformní klastry ke spuštění více správců front se stejnou konfigurací. To má další

výhodu, že se snižuje dopad restartování jednoho kontejneru (například v rámci údržby kontejnerové platformy).

CP4I-LTS OpenShift CP4I CD Použití IBM MQ Operator pro Red Hat OpenShift

IBM MQ Operator implementuje a spravuje IBM MQ jako součást produktu IBM Cloud Pak for Integration nebo samostatně v produktu Red Hat OpenShift Container Platform

Procedura

- “Historie vydání pro IBM MQ Operator” na stránce 34.
- “Migrace IBM MQ do produktu IBM Cloud Pak for Integration” na stránce 79.
- “Instalace produktu IBM MQ Operator” na stránce 101.
- “Upgrade produktu IBM MQ Operator a správců front” na stránce 119.
- “Implementace správce front do klastru Red Hat OpenShift Container Platform” na stránce 114.
- “Provozování produktu IBM MQ pomocí IBM MQ Operator” na stránce 168.
- “Odkaz rozhraní API pro IBM MQ Operator” na stránce 179.

CP4I-LTS OpenShift CP4I CD Historie vydání pro IBM MQ Operator

Notes:

- Informace o dřívějších operátorech systému IBM MQ naleznete v části Historie vydání produktu IBM MQ Operator v dokumentaci k produktu IBM MQ 9.2 .
- Chcete-li získat informace o budoucích aktualizacích produktu IBM MQ , prohlédněte si celkovou stránku IBM MQ data plánovaného vydání údržby .

IBM MQ Operator 3.1.3

CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.4.1

Kanál operátoru
`v3.1`

Přípustné hodnoty pro `.spec.version`
9.3.5.1-r2

Povolené hodnoty pro `.spec.version` během migrace
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3,9.3.3.2-r3 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1, 9.3.0.17-r2, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1, 9.3.3.3-r2, 9.3.4.0-r1, 9.3.4.1-r1, 9.3.5.0-r1, 9.3.5.0-r2, 9.3.5.1-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 4.3 a vyšší (volitelná instalace).

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 3.1.2

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.4.1

Kanál operátoru
`v3.1`

Přípustné hodnoty pro `.spec.version`
9.3.5.1-r1

Povolené hodnoty pro `.spec.version` během migrace
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3,9.3.3.2-r3 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1, 9.3.3.3-r2, 9.3.4.0-r1, 9.3.4.1-r1, 9.3.5.0-r1, 9.3.5.0-r2,

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 4.3 a vyšší (volitelná instalace).

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 3.1.1

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.4.1

Kanál operátoru
`v3.1`

Přípustné hodnoty pro `.spec.version`
9.3.5.0-r2

Povolené hodnoty pro `.spec.version` během migrace
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3,9.3.3.2-r3 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1, 9.3.3.3-r2, 9.3.4.0-r1, 9.3.4.1-r1, 9.3.5.0-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 4.3 a vyšší (volitelná instalace).

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 3.1.0

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.4.1

Kanál operátoru
`v3.1`

Přípustné hodnoty pro `.spec.version`
9.3.5.0-r1

Povolené hodnoty pro `.spec.version` během migrace
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3,9.3.3.2-r3 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1, 9.3.3.3-r2, 9.3.4.0-r1, 9.3.4.1-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 4.3 a vyšší (volitelná instalace).

Změny

- Chyby zabezpečení, které jsou adresovány, jsou podrobně popsány v těchto bulletinech zabezpečení:
  - https://www.ibm.com/support/pages/node/7126571.
  - https://www.ibm.com/support/pages/node/7137570.

IBM MQ Operator 3.0.1

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.4.1

Kanál operátoru
`v3.0`

Přípustné hodnoty pro `.spec.version`
9.3.4.1-r1

Povolené hodnoty pro `.spec.version` během migrace
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3,9.3.3.2-r3 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1, 9.3.4.0-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 4.3 a vyšší (volitelná instalace).

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 3.0.0” na stránce 37.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 3.0.0

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.4.1

Kanál operátoru
`v3.0`

Přípustné hodnoty pro `.spec.version`
9.3.4.0-r1

Povolené hodnoty pro `.spec.version` během migrace
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 4.3 a vyšší (volitelná instalace).

Novinky

- Webový server IBM MQ můžete nakonfigurovat přidáním souboru `mqwebuser.xml` do ConfigMap nebo Secret pomocí nové vlastnosti `manualConfig` YAML (vyžaduje IBM MQ 9.3.4 nebo vyšší).
- Produkt administrative REST API je nyní podporován. Tuto konfiguraci můžete nakonfigurovat prostřednictvím ConfigMap nebo Secret (vyžaduje verzi IBM MQ 9.3.4 nebo vyšší). Mějte však na paměti, že webový server stále není považován za kritickou službu pro zkoušku životnosti, takže pokud selže, kontejner nebude automaticky restartován.
- Jednotné přihlášení zakážete při použití licence na produkt IBM Cloud Pak for Integration výběrem volby "ruční" ověření a autorizace (vyžaduje produkt IBM MQ 9.3.4 nebo vyšší).
- V kontejneru můžete povolit kořenový systém souborů jen pro čtení. To zlepšuje zabezpečení tím, že brání zápisu do většiny souborů v kontejneru za běhu (vyžaduje verzi IBM MQ 9.3.4 nebo vyšší). Volba `readOnlyRootFilesystem` je doplněna dalšími volbami pro konfiguraci velikosti svazků "pracovní" a "tmp", které jsou připojeny, aby umožňovaly zápis dočasných souborů. Viz “Spuštění kontejneru IBM MQ s kořenovým systémem souborů jen pro čtení” na stránce 165.

Změny

- Odebrané (dříve zamítnuté) verze: IBM MQ 9.2.0 EUS, 9.2.3, 9.2.4, 9.2.5. Důležité: Před upgradem produktu IBM MQ Operatorse ujistěte, že nemáte správce front pro žádnou z odebraných verzí. Po upgradu již nebudete moci upravovat prostředek QueueManager , jinak než upgradovat na podporovanou verzi, protože produkt IBM MQ Operator již starší verze nerozpoznává.
- Instalace a životní cyklus operátora
  - Produkt IBM MQ Operator je nyní podporován na systému Red Hat OpenShift Container Platform verze 4.14.
  - IBM MQ Operator Již neinstaluje IBM Cloud Pak foundational services automaticky. Pokud implementujete QueueManager , který používá licenci IBM Cloud Pak for Integration a který konfiguruje jednotné přihlášení (výchozí pro správce front s touto licencí), QueueManager přejde do stavu "Blokováno", pokud nezbytné závislosti již nejsou nainstalovány. Žádný jiný operátor nebude nainstalován automaticky.
- Změny zabezpečení
  - Produkt IBM Cloud Pak for Integration 2023.4.1 používá produkt Keycloak pro jednotné přihlášení a autorizaci namísto produktu IBM Cloud Pak Identity and Access Manager.

  - Šablona IBM Cloud Pak for Integration "quick start" již nezakazuje zabezpečení s aplikací *MQSNOAUT*. Musíte nakonfigurovat ověření. Viz téma “Ověření uživatele a autorizace pro produkt IBM MQ v kontejnerech” na stránce 28.
  - Zakázaní výchozí uživatelé v produktu IBM MQ Advanced for Developers z verze 9.3.4. Výchozí uživatelé ("admin" a "app") a další konfigurace poskytované jako součást produktu IBM MQ Advanced for Developers jsou standardně zakázány.
- Vedlejší změny v sekci IBM MQ Operator :
  - Produkt IBM MQ Operator již neimplementuje inicializační kontejner
  - Název kontejneru IBM MQ Operator je nyní *manager* .
  - Předpona sekce IBM MQ Operator je *ibm-mq-operator* .
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.4.8

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.3.3.3-r2

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Chyby zabezpečení, které jsou adresovány, jsou podrobně popsány v těchto bulletinech zabezpečení:
  - https://www.ibm.com/support/pages/node/7126571.
  - https://www.ibm.com/support/pages/node/7137570.

IBM MQ Operator 2.4.7

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.3.3.3-r1

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.4.6

CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.4.5

CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1,

9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.4.4

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.
- Produkt IBM MQ Operator již není testován nebo podporován na systému OpenShift Container Platform 4.10.

IBM MQ Operator 2.4.3

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1,

9.3.0.10-r2, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.4.2

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.4.1

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.4.0” na stránce 42.
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.4.0

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2023.2.1

Kanál operátoru
`v2.4`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Novinky

- Byla odebrána integrace řídicího panelu operací.
- Přidána IBM MQ Operator podpora pro **`LogFilePages`**.

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.3.3

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.4.1

Kanál operátoru
`v2.3`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému "IBM MQ Operator 2.3.0" na stránce 44
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.3.2

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.4.1

Kanál operátoru
`v2.3`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému "IBM MQ Operator 2.3.0" na stránce 44
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.3.1

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.4.1

Kanál operátoru
`v2.3`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Novinky

- Od března 2023 jsou obrazy kontejnerů IBM MQ Operator a IBM MQ správce front digitálně podepsány. Obrazy IBM MQ Operator 2.3.1 a IBM MQ 9.3.2.0-r2 byly podepsány s tímto vydáním. Viz téma "Ověřování podpisů obrázků" na stránce 78.

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému "IBM MQ Operator 2.3.0" na stránce 44
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.3.0

CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.4.1

Kanál operátoru
`v2.3`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Novinky

- Od verze IBM MQ Operator 2.3.0lze konfigurovat podporu FIPS 140-2. Viz téma "Shoda s FIPS pro IBM MQ v kontejnerech" na stránce 30.
- Od verze IBM MQ Operator 2.3.0je produkt IBM MQ 9.3.1 zamítnutý.

Změny

- Od verze IBM MQ Operator 2.3.0je produkt "Nativní vysoká dostupnost" na stránce 141 k dispozici pod licencí IBM MQ Advanced nebo IBM MQ Advanced for Developers .
- Sada oprávnění vyžadovaných produktem IBM MQ Operator je omezena.
- Z produktu IBM MQ Operator 2.3.0se **`ibm-automation-core`** odebere z `OperandRequest` provedených pro IBM Cloud Pak for Integration implementace.
- Od verze IBM MQ Operator 2.3.0implementace IBM MQ Operator uvádí **`imagePullPolicy`** z `IfNotPresent`.
- Chyby zabezpečení, které jsou adresovány, jsou podrobně popsány v těchto vývěsech zabezpečení:
  - Vývěska pro CVE-2022-47629 a CVE-2022-35737
  - Vývěska pro CVE-2023-26284

IBM MQ Operator 2.2.2

CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.4.1

Kanál operátoru
`v2.2`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.2.1

CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.4.1

Kanál operátoru
`v2.2`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.2.0

CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.4.1

Kanál operátoru
`v2.2`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.1.0-r1, 9.3.1.0-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services verze 3.19 až 3.24 včetně.

Novinky

- Od verze IBM MQ Operator 2.2.0 (CD) je trasování IBM Instana podporováno nativně. Podpora je k dispozici v obrazu kontejneru správce front 9.3.1.0-r2 (CD) IBM MQ . 9.3.1.0-r2 obsahuje verzi 2.4.0 (2022.4.0) uživatelské procedury IBM Instana MQ Exit. Chcete-li povolit trasování IBM Instana , viz “Integrace produktu IBM MQ s trasováním IBM Instana” na stránce 155.

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.
- Od verze IBM MQ Operator 2.2.0je řídicí panel operací zamítnutý a neobdrží žádné další aktualizace. Neměla by být spuštěna žádná nová použití řídicího panelu operací. IBM MQ 2.0.x Operátoři nadále podporují řídicí panel operací.

IBM MQ Operator 2.1.0

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.1`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.1.0-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.X, ale alespoň 3.19

Novinky

- Přidá IBM MQ 9.3.1.
- Přidá novou volbu, která uživatelům umožňuje zakázat aktualizace výchozích hodnot specifikace správce front.
- Přidá novou podmínku stavu, která zamítne všechny verze produktu IBM MQ starší než IBM MQ 9.3.1.
- Přidá novou podmínku stavu, která varuje uživatele, kteří používají operandy LTS s touto verzí disku CD produktu IBM MQ Operator.

Změny

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.23 (LTS)

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.3.0.17-r3

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1, 9.3.0.17-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace zabezpečení sestavená na “IBM MQ Operator 2.0.0” na stránce 57
- IBM MQ Obraz katalogu byl přesunut do formátu katalogu založeného na souboru z formátu databáze SQLite .
- Ohrožení zabezpečení, která jsou adresována, jsou podrobně popsána v tomto Věstníku zabezpečení .

IBM MQ Operator 2.0.22 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.3.0.17-r2

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Ohrožení zabezpečení, která jsou adresována, jsou podrobně popsána v tomto Věstníku zabezpečení .

IBM MQ Operator 2.0.21 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.3.0.17-r1

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Ohrožení zabezpečení, která jsou adresována, jsou podrobně popsána v tomto Věstníku zabezpečení .

IBM MQ Operator 2.0.20 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.3.0.16-r2

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Ohrožení zabezpečení, která jsou adresována, jsou podrobně popsána v tomto Věstníku zabezpečení .

IBM MQ Operator 2.0.19 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.3.0.16-r1

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Chyby zabezpečení, které jsou adresovány, jsou podrobně popsány v těchto bulletinech zabezpečení:
  - https://www.ibm.com/support/pages/node/7126571.
  - https://www.ibm.com/support/pages/node/7137570.

IBM MQ Operator 2.0.18 (LTS)

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.3.0.15-r1

Povolené hodnoty pro `.spec.version` během migrace
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.17 (LTS)

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
v2.0

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.
- Produkt IBM MQ Operator již není testován nebo podporován na systému OpenShift Container Platform 4.10.

IBM MQ Operator 2.0.16 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
v2.0

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.12 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.
- Produkt IBM MQ Operator již není testován nebo podporován na systému OpenShift Container Platform 4.10.

IBM MQ Operator 2.0.15 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.14 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.13 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.12 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.11 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.10 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.9 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Novinky

- Od března 2023 jsou obrazy kontejnerů IBM MQ Operator a IBM MQ správce front digitálně podepsány. Obrazy IBM MQ Operator 2.0.9 a IBM MQ 9.3.0.4-r2 byly podepsány s tímto vydáním. Viz “Ověřování podpisů obrázků” na stránce 78)

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.8 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Chyby zabezpečení, které jsou adresovány, jsou podrobně popsány v těchto vývěsech zabezpečení:
  - Vývěska pro CVE-2022-47629 a CVE-2022-35737
  - Vývěska pro CVE-2023-26284

IBM MQ Operator 2.0.7 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.6 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.5 (LTS)

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.4

CP4I-LTS

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.3

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.0.6-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.2

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.0.6-r2-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57

- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.1

CP4I-LTS CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.0.6-r1-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1, 9.3.0.0-r2

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Změny

- Aktualizace pouze pro zabezpečení sestavená na systému “IBM MQ Operator 2.0.0” na stránce 57
- Zranitelnosti, které jsou řešeny, jsou podrobně popsány na této Vývěsce o zabezpečení.

IBM MQ Operator 2.0.0

CP4I-LTS CD

Verze IBM Cloud Pak for Integration
IBM Cloud Pak for Integration 2022.2.1

Kanál operátoru
`v2.0`

Přípustné hodnoty pro `.spec.version`
9.2.0.1-r1-eus, 9.2.0.2-r1-eus, 9.2.0.2-r2-eus, 9.2.0.4-r1-eus, 9.2.0.5-r1-eus, 9.2.0.5-r2-eus, 9.2.0.5-r3-eus, 9.2.3.0-r1, 9.2.4.0-r1, 9.2.5.0-r1, 9.2.5.0-r2, 9.2.5.0-r3, 9.3.0.0-r1

Verze Red Hat OpenShift Container Platform
OpenShift Container Platform 4.10 a vyšší. **Poznámka**: Podporovány jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.10 a 4.12.

Verze IBM Cloud Pak foundational services
IBM Cloud Pak foundational services 3.19

Novinky

- Přidá IBM MQ 9.3.0.
- Přidává podporu pro POWER (ppc64le).

Změny

- Red Hat OpenShift Container Platform 4.10 se nyní požaduje. Viz téma “Podpora verze pro IBM MQ Operator” na stránce 11.
- Deprecated Zamítnuté verze: IBM MQ 9.2.3. Tyto verze nemusí být sladěny s budoucími verzemi produktu IBM MQ Operator.
- Removed Odebrané (dříve zamítnuté) verze průběžného doručení: IBM MQ 9.1.5, 9.2.0 CD, 9.2.1, 9.2.2

- Ověření IBM MQ Operator webového háčku je nyní instalováno produktem Operator Lifecycle Manager (OLM). OLM nyní spravuje certifikát webového háčku.
- Opravena chyba, která dříve generovala varování uživatelských předvoleb v protokolování IBM MQ Console .
- Chyby zabezpečení, které jsou adresovány, jsou podrobně popsány v těchto bulletinech zabezpečení:
  - https://www.ibm.com/support/pages/node/6602255
  - https://www.ibm.com/support/pages/node/6602259

CP4I-LTS OpenShift CP4I CD Historie vydání pro obrazy kontejneru správce front pro použití s produktem IBM MQ Operator

Poznámka: Informace o předchozích obrazech kontejneru správce front naleznete v tématu Historie vydání pro produkt IBM MQ Operator v dokumentaci k produktu IBM MQ 9.2 .

9.3.5.1-r2

CD

Požadovaná verze operátoru
3.1.3 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.5.1-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.5.1-r2`
- `icr.io/ibm-messaging/mq:9.3.5.1-r2`

Novinky

- Novinky v IBM MQ 9.3.5

Změny

- Co se změnilo v IBM MQ 9.3.5
- Založeno na Red Hat Universal Base Image 8.9-1161.1715068733
- Knihovna golang.org/x/net byla upgradována, aby napravila ohlášenou zranitelnost

9.3.5.1-r1

CD

Požadovaná verze operátoru
3.1.2 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.5.1-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.5.1-r1`
- `icr.io/ibm-messaging/mq:9.3.5.1-r1`

Novinky

- Novinky v IBM MQ 9.3.5

Změny

- Co se změnilo v IBM MQ 9.3.5
- Založeno na Red Hat obrazu Universal Base 8.9-1161
- "dependabot" hlášeny bezpečnostní chyby byly řešeny

9.3.5.0-r2

CD

Požadovaná verze operátoru
3.1.1 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.5.0-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.5.0-r2`
- `icr.io/ibm-messaging/mq:9.3.5.0-r2`

Novinky

- Novinky v IBM MQ 9.3.5

Změny

- Co se změnilo v IBM MQ 9.3.5
- Založeno na Red Hat Univerzální základní obraz 8.9-1137
- Nový obrázek 9.3.5.0-r2 je třeba vyzvednout pouze v případě, že máte povolen řídicí panel operací.

9.3.5.0-r1

CD

Požadovaná verze operátoru
3.1.0 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.5.0-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.5.0-r1`
- `icr.io/ibm-messaging/mq:9.3.5.0-r1`

Novinky

- Novinky v IBM MQ 9.3.5

Změny

- Co se změnilo v IBM MQ 9.3.5
- Založeno na Red Hat Univerzální základní obraz 8.9-1137
- Symbolický odkaz je poskytnut pro `/var/mam` , kde by se zkopírovala nešifrovaná pověření v `mqwebuser.xml` .
- Knihovna golang.org/x/crypto byla upgradována pro nápravu ohrožení zabezpečení CVE-2023-48795 .
- Bezpečnější algoritmus SHA512 použitý místo SHA256 k vytvoření certifikátu podepsaného držitelem ve webovém úložišti klíčů.

- Úložiště klíčů PKCS#12 pro použití s webovým serverem IBM MQ je nyní generováno pomocí funkce **Pkcs12.Modern.Encode** , která používá šifrování SHA-2 (dříve generované pomocí staršího šifrování SHA-1).
- Zranitelnost hlášená při použití metody **PathTraversal** je opravena.

9.3.4.1-r1

CD

Požadovaná verze operátoru
3.0.1 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.4.1-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.4.1-r1`
- `icr.io/ibm-messaging/mq:9.3.4.1-r1`

Novinky

- Novinky v IBM MQ 9.3.4

Změny

- Co se změnilo v IBM MQ 9.3.4
- Založeno na Red Hat Universal Base Image 8.9-1108

9.3.4.0-r1

CD

Požadovaná verze operátoru
3.0.0 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.4.0-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.4.0-r1`
- `icr.io/ibm-messaging/mq:9.3.4.0-r1`

Novinky

- Novinky v IBM MQ 9.3.4

Změny

- Co se změnilo v IBM MQ 9.3.4
- Založeno na Red Hat Univerzální základní obraz 8.9-1029
- Vylepšená podpora webového serveru IBM MQ -Protokol webového serveru IBM MQ se nyní standardně zobrazuje v protokolu kontejneru. Soubor `messages.log` webového serveru je nyní automaticky zrcadlen do výstupu protokolu kontejneru. V rámci této změny je nyní soubor `messages.log` zapsaný na disk vždy ve formátu JSON, ačkoli protokol kontejneru je nadále k dispozici buď jako formát JSON, nebo jako "základní" formát čitelný pro člověka.
- Byla opravena obsluha signálu v obrazu kontejneru správce front tak, aby správně zpracovala řídicí signály v případě, že je kontejner ukončen produktem Red Hat OpenShift Container Platform před dokončením spuštění.

9.3.3.3-r2

Požadovaná verze operátoru
2.4.8 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.3-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.3-r2`
- `icr.io/ibm-messaging/mq:9.3.3.3-r2`

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Univerzální základní obraz 8.9-1137
- Knihovna golang.org/x/crypto byla upgradována pro nápravu ohrožení zabezpečení CVE-2023-48795 .
- Bezpečnější algoritmus SHA512 použitý místo SHA256 k vytvoření certifikátu podepsaného držitelem ve webovém úložišti klíčů.
- Úložiště klíčů PKCS#12 pro použití s webovým serverem IBM MQ je nyní generováno pomocí funkce **`Pkcs12.Modern.Encode`** , která používá šifrování SHA-2 (dříve generované pomocí staršího šifrování SHA-1).
- Zranitelnost hlášená při použití metody **`PathTraversal`** je opravena.

9.3.3.3-r1

Požadovaná verze operátoru
2.4.7 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.3-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.3-r1`
- `icr.io/ibm-messaging/mq:9.3.3.3-r1`

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Universal Base Image 8.9-1108

IBM MQ včetně oprav APAR

- IT44961
- IT44821
- IT44954

9.3.3.2-r3

CD

Požadovaná verze operátoru
2.4.6 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.2-r3`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.2-r3`
- `icr.io/ibm-messaging/mq:9.3.3.2-r3`

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Univerzální základní obraz 8.9-1029

9.3.3.2-r2

CD

Požadovaná verze operátoru
2.4.5 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.2-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.2-r2`
- `icr.io/ibm-messaging/mq:9.3.3.2-r2`

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Universal Base Image 8.8-1072.1697626218
- IBM MQ Obraz kontejneru správce front 9.3.3.2-r2 obsahuje verzi 3.1.7 (2023.4.0) produktu Instana MQ Exit.

9.3.3.2-r1

CD

Požadovaná verze operátoru
2.4.4 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.2-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.2-r1`
- `icr.io/ibm-messaging/mq:9.3.3.2-r1`

Novinky

- Novinky v IBM MQ 9.3.3

Změny
[5]

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Universal Base Image 8.8-1072.1697626218
- Aktualizuje úroveň knihovny libcurl na 8.4.0.

IBM MQ včetně oprav APAR

- IT41871
- IT44585
- IT44623
- IT44762

9.3.3.1-r2

CD

Požadovaná verze operátoru
2.4.3 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.1-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.1-r2`
- `icr.io/ibm-messaging/mq:9.3.3.1-r2`

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.3.1-r1
- Založeno na Red Hat Universal Base Image 8.8-1037

9.3.3.1-r1

CD

Požadovaná verze operátoru
2.4.2 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.1-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.1-r1`
- `icr.io/ibm-messaging/mq:9.3.3.1-r1`

[5] Předchozí verze tohoto tématu nesprávně uvedla, že IBM MQ obraz kontejneru správce front 9.3.3.2-r1 obsahuje verzi 3.1.7 (2023.4.0) procedury Instana MQ Exit.

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Universal Base Image 8.8-1037.

9.3.3.0-r2

Požadovaná verze operátoru
2.4.1 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.0-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.0-r2`
- `icr.io/ibm-messaging/mq:9.3.3.0-r2`

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Universal Base Image 8.8-1014.

9.3.3.0-r1

Požadovaná verze operátoru
2.4.0 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.3.0-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.3.0-r1`
- `icr.io/ibm-messaging/mq:9.3.3.0-r1`

Novinky

- Novinky v IBM MQ 9.3.3

Změny

- Co se změnilo v IBM MQ 9.3.3
- Založeno na Red Hat Universal Base Image 8.8-860.
- IBM MQ Obraz kontejneru správce front 9.3.3.0-r1 zahrnuje verzi 3.1.2 (2023.2.0) uživatelské procedury MQ Exit.

9.3.2.1-r2

Požadovaná verze operátoru
2.3.3 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.2.1-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.2.1-r2`
- `icr.io/ibm-messaging/mq:9.3.2.1-r2`

Novinky

- Novinky v IBM MQ 9.3.2

Změny

- Co se změnilo v IBM MQ 9.3.2
- Založeno na Red Hat Universal Base Image 8.7-1107.

9.3.2.1-r1

CD

Požadovaná verze operátoru
2.3.2 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.2.1-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.2.1-r1`
- `icr.io/ibm-messaging/mq:9.3.2.1-r1`

Novinky

- Novinky v IBM MQ 9.3.2

Změny

- Co se změnilo v IBM MQ 9.3.2
- Založeno na Red Hat Universal Base Image 8.7-1107.

9.3.2.0-r2

CD

Požadovaná verze operátoru
2.3.1 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.2.0-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.2.0-r2`
- `icr.io/ibm-messaging/mq:9.3.2.0-r2`

Novinky

- Novinky v IBM MQ 9.3.2

Změny

- Co se změnilo v IBM MQ 9.3.2
- Založeno na Red Hat Universal Base Image 8.7-1085.

9.3.2.0-r1

CD

Požadovaná verze operátoru
2.3.0 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.2.0-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.2.0-r1`
- `icr.io/ibm-messaging/mq:9.3.2.0-r1`

Novinky

- Novinky v IBM MQ 9.3.2
- Nyní je nastavena proměnná prostředí *MQ_LOGGING_CONSOLE_FORMAT* , která nahrazuje zamítnutou proměnnou *LOG_FORMAT* .

Změny

- Co se změnilo v IBM MQ 9.3.2
- Certifikáty správce front se stejným rozlišujícím názvem subjektu (DN) jako certifikát vydavatele (CA) nejsou podporovány. Certifikát musí mít jedinečný rozlišující název subjektu.
- Založeno na Red Hat Universal Base Image 8.7-1049.1675784874.

9.3.1.1-r1

CD

Požadovaná verze operátoru
2.2.2 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.1.1-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.1.1-r1`
- `icr.io/ibm-messaging/mq:9.3.1.1-r1`

Novinky

- Novinky v IBM MQ 9.3.1

Změny

- Co se změnilo v IBM MQ 9.3.1
- Založeno na Red Hat Universal Base Image 8.7-1031.
- IBM MQ Obraz kontejneru správce front 9.3.1.1-r1 zahrnuje verzi 2.4.3 (2022.4.3) produktu IBM Instana MQ Exit.

9.3.1.0-r3

CD

Požadovaná verze operátoru
2.2.1 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.1.0-r3`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.1.0-r3`
- `icr.io/ibm-messaging/mq:9.3.1.0-r3`

Novinky

- Novinky v IBM MQ 9.3.1

Změny

- Co se změnilo v IBM MQ 9.3.1
- Založeno na Red Hat Universal Base Image 8.7-923.1669829893.
- IBM MQ Obraz kontejneru správce front 9.3.1.0-r3 zahrnuje verzi 2.4.3 (2022.4.3) produktu IBM Instana MQ Exit.

9.3.1.0-r2

CD

Požadovaná verze operátoru
2.2.0 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.1.0-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.1.0-r2`
- `icr.io/ibm-messaging/mq:9.3.1.0-r2`

Novinky

- Novinky v IBM MQ 9.3.1
- Z obrazu 9.3.1.0-r2 (CD) IBM MQ Kontejner správce front je nativní trasování IBM Instana podporováno. IBM MQ verze 9.3.1.0-r2 zahrnuje verzi 2.4.0 (2022.4.0) uživatelské procedury IBM Instana MQ Exit. Chcete-li povolit trasování IBM Instana , viz “Integrace produktu IBM MQ s trasováním IBM Instana” na stránce 155.

Změny

- Co se změnilo v IBM MQ 9.3.1
- Založeno na Red Hat Universal Base Image 8.7-923.
- Pokud klíč a certifikát nejsou zadány, atribut správce front **SSLKEYR** je nyní nastaven na prázdnou hodnotu, nikoli na hodnotu "`/run/runmqserver/tls/key`".

9.3.1.0-r1

CD

Požadovaná verze operátoru
2.1.0 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.1.0-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.1.0-r1`
- `icr.io/ibm-messaging/mq:9.3.1.0-r1`

Novinky

- Novinky v IBM MQ 9.3.1

Změny

- Co se změnilo v IBM MQ 9.3.1
- Založeno na Red Hat Universal Base Image 8.6-941.

9.3.0.17-r3

CP4I-LTS

Požadovaná verze operátoru
2.0.22 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.17-r3`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.17-r3`
- `icr.io/ibm-messaging/mq:9.3.0.17-r3`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 9.4-949.1716471857

9.3.0.17-r2

CP4I-LTS

Požadovaná verze operátoru
2.0.22 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.17-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.17-r2`
- `icr.io/ibm-messaging/mq:9.3.0.17-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace zabezpečení sestavená na IBM MQ 9.3.0.0-r1

- Založeno na Red Hat Universal Base Image 8.9-1161.1715068733
- Knihovna golang.org/x/net byla upgradována, aby napravila ohlášenou zranitelnost

9.3.0.17-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.21 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.17-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.17-r1`
- `icr.io/ibm-messaging/mq:9.3.0.17-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace zabezpečení sestavená na IBM MQ 9.3.0.0-r1
- Založeno na Red Hat obrazu Universal Base 8.9-1161
- "dependabot" hlášeny bezpečnostní chyby byly řešeny.

9.3.0.16-r2

CP4I-LTS

Požadovaná verze operátoru
2.0.20 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.16-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.16-r2`
- `icr.io/ibm-messaging/mq:9.3.0.16-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace zabezpečení sestavená na IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Univerzální základní obraz 8.9-1137
- Nový obrázek 9.3.0.16-r2 je třeba vyzvednout pouze v případě, že máte povolen řídicí panel operací.

9.3.0.16-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.19 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.16-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.16-r1`
- `icr.io/ibm-messaging/mq:9.3.0.16-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace zabezpečení sestavená na IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Univerzální základní obraz 8.9-1137
- Knihovna golang.org/x/crypto byla upgradována pro nápravu ohrožení zabezpečení CVE-2023-48795 .
- Bezpečnější algoritmus SHA512 použitý místo SHA256 k vytvoření certifikátu podepsaného držitelem ve webovém úložišti klíčů.
- Úložiště klíčů PKCS#12 pro použití s webovým serverem IBM MQ je nyní generováno pomocí funkce **`Pkcs12.Modern.Encode`** , která používá šifrování SHA-2 (dříve generované pomocí staršího šifrování SHA-1).
- Zranitelnost hlášená při použití metody **`PathTraversal`** je opravena.

9.3.0.15-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.18 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.15-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.15-r1`
- `icr.io/ibm-messaging/mq:9.3.0.15-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.9-1108

9.3.0.11-r2

CP4I-LTS

Požadovaná verze operátoru
2.0.17 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.11-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.11-r2`
- `icr.io/ibm-messaging/mq:9.3.0.11-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.9-1029.

9.3.0.11-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.16 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.11-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.11-r1`
- `icr.io/ibm-messaging/mq:9.3.0.11-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.8-1072.1697626218.
- Aktualizuje úroveň knihovny libcurl na 8.4.0

9.3.0.10-r2

CP4I-LTS

Požadovaná verze operátoru
2.0.15 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.10-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.10-r2`
- `icr.io/ibm-messaging/mq:9.3.0.10-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.8-1037.

9.3.0.10-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.14 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.10-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.10-r1`
- `icr.io/ibm-messaging/mq:9.3.0.10-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.8-1037.

9.3.0.6-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.13 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.6-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.6-r1`
- `icr.io/ibm-messaging/mq:9.3.0.6-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.8-1014.

9.3.0.5-r3

CP4I-LTS

Požadovaná verze operátoru
2.0.12 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.5-r3`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.5-r3`
- `icr.io/ibm-messaging/mq:9.3.0.5-r3`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.8-860.

9.3.0.5-r2

CP4I-LTS

Požadovaná verze operátoru
2.0.11 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.5-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.5-r2`
- `icr.io/ibm-messaging/mq:9.3.0.5-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.7-1107.

Důležité: Pro uživatele panelu dashboard operací na serveru IBM MQ LTS Obraz kontejneru správce front 9.3.0.5-r2

Je-li povolen řídicí panel operací, IBM MQ LTS Obraz kontejneru správce front 9.3.0.5-r2 nasadí produkt Operations Dashboard Agent a obrazy kolektoru, které neobsahují nejnovější opravy zabezpečení dostupné v době jejich obecné dostupnosti.

Zmírnění: Proveďte upgrade alespoň na 9.3.0.5-r3 všechny obrazy IBM MQ LTS Kontejner správce front 9.3.0.5-r2 s povoleným řídicím panelem operací. Viz téma “Upgrade správce front IBM MQ pomocí Red Hat OpenShift” na stránce 129.

9.3.0.5-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.10 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.5-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.5-r1`
- `icr.io/ibm-messaging/mq:9.3.0.5-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.7-1107.

Důležité: Pro uživatele řídicího panelu operací na IBM MQ LTS Obraz kontejneru správce front 9.3.0.5-r1

Je-li povolen řídicí panel operací, IBM MQ LTS Obraz kontejneru správce front 9.3.0.5-r1 nasadí obrazy produktu Operations Dashboard Agent a Collector, které neobsahují nejnovější opravy zabezpečení dostupné v době jejich obecné dostupnosti.

Zmírnění: Proveďte upgrade alespoň na 9.3.0.5-r3 všechny obrazy IBM MQ LTS Kontejner správce front 9.3.0.5-r1 s povoleným řídicím panelem operací. Viz téma "Upgrade správce front IBM MQ pomocí Red Hat OpenShift" na stránce 129.

9.3.0.4-r2

CP4I-LTS

Požadovaná verze operátoru
2.0.9 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.4-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.4-r2`
- `icr.io/ibm-messaging/mq:9.3.0.4-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.7-1085.

9.3.0.4-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.8 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.4-r1`

- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.4-r1`
- `icr.io/ibm-messaging/mq:9.3.0.4-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.7-1049.1675784874.

9.3.0.3-r1

CP4I-LTS

Požadovaná verze operátoru
2.0.7 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.3-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.3-r1`
- `icr.io/ibm-messaging/mq:9.3.0.3-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.7-1031.

9.3.0.1-r4

CP4I-LTS

Požadovaná verze operátoru
2.0.6 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.1-r4`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.1-r4`
- `icr.io/ibm-messaging/mq:9.3.0.1-r4`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.7-923.1669829893.

9.3.0.1-r3

CP4I-LTS

Požadovaná verze operátoru
2.0.5 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.1-r3`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.1-r3`
- `icr.io/ibm-messaging/mq:9.3.0.1-r3`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.7-923.

9.3.0.1-r2

CP4I-LTS

Požadovaná verze operátoru
2.0.4 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.1-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.1-r2`
- `icr.io/ibm-messaging/mq:9.3.0.1-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.6-941.

9.3.0.1-r1

CP4I-LTS CD

Požadovaná verze operátoru
2.0.3 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.1-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.1-r1`

- `icr.io/ibm-messaging/mq:9.3.0.1-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.6-941.

9.3.0.0-r3

Požadovaná verze operátoru
2.0.2 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.0-r3`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.0-r3`
- `icr.io/ibm-messaging/mq:9.3.0.0-r3`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.6-902.

9.3.0.0-r2

Požadovaná verze operátoru
2.0.1 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.0-r2`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.0-r2`
- `icr.io/ibm-messaging/mq:9.3.0.0-r2`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Aktualizace pouze pro zabezpečení sestavená na systému IBM MQ 9.3.0.0-r1
- Založeno na Red Hat Universal Base Image 8.6-854.

9.3.0.0-r1

CP4I-LTS CD

Požadovaná verze operátoru
2.0.0 nebo vyšší

Podporované architektury
amd64, s390x, ppc64le

Obrázky

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.3.0.0-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.3.0.0-r1`
- `icr.io/ibm-messaging/mq:9.3.0.0-r1`

Novinky

- Novinky v IBM MQ 9.3.0

Změny

- Co se změnilo v IBM MQ 9.3.0
- Výchozí konfigurace vývojáře v obrazu MQ Advanced for Developers nyní používá `ANY_TLS12_OR_HIGHER`.
- Opraven problém s webovým serverem IBM MQ , který způsobil chybu v protokolu kvůli chybějícím předvolbám Java .
- Založeno na Red Hat Universal Base Image 8.6-751.1655117800.

OpenShift CP4I Ověřování podpisů obrázků

Od března 2023 jsou obrazy kontejnerů IBM MQ Operator a IBM MQ správce front digitálně podepsány.

První operátor IBM MQ , který má být podepsán:

- 2.3.1 (CD)
- 2.0.9 (LTS)

První obrazy kontejneru správce front IBM MQ , které mají být podepsány:

- 9.3.2.0-r2 (CD)
- 9.3.0.4-r2 (LTS)

Informace o této úloze

Digitální podpisy poskytují spotřebitelům obsahu způsob, jak zajistit, že to, co si stáhnou, je autentické (pochází z očekávaného zdroje) a má integritu (to je to, co očekáváme, že to bude).

Procedura

- Ověřte podpisy obrazů kontejneru IBM MQ Operator a IBM MQ správce front:
  - V 9.3.4 Operator3.0.0 Informace o produktu IBM MQ Operator na adrese 3.0.0 nebo novější nebo o obrazu kontejneru správce front IBM MQ na adrese 9.3.4.0-r1 nebo novější naleznete v části Ověření podpisů obrazů v dokumentaci k produktu IBM Cloud Pak for Integration (CP4I) 2023.4 .
  - Operator2.4.0 V případě IBM MQ Operator na adrese 2.4.xnebo obrazu kontejneru správce front IBM MQ na adrese 9.3.3.xviz téma Ověření podpisů obrazů v dokumentaci k produktu CP4I 2023.2 .
  - Informace o produktu IBM MQ Operator před verzí 2.4.0nebo o obrazu kontejneru správce front IBM MQ před verzí 9.3.3.0-r1naleznete v tématu Ověřování podpisů obrazů v dokumentaci k produktu CP4I 2022.4 .

CP4I-LTS OpenShift CD Migrace IBM MQ do produktu IBM Cloud Pak for Integration

Tato sada témat popisuje klíčové kroky k migraci stávajícího správce front IBM MQ do prostředí kontejneru pomocí IBM MQ Operator v IBM Cloud Pak for Integration.

Informace o této úloze

Klienti, kteří implementují produkt IBM MQ na serveru Red Hat OpenShift, lze rozdělit do následujících scénářů:

1. Vytvoření nové implementace IBM MQ v Red Hat OpenShift pro nové aplikace.
2. Rozšíření sítě IBM MQ do Red Hat OpenShift pro nové aplikace v Red Hat OpenShift.
3. Přesunutí implementace IBM MQ do Red Hat OpenShift bude pokračovat v podpoře existujících aplikací.

To platí pouze pro scénář 3, který potřebujete k migraci konfigurace produktu IBM MQ. Ostatní scénáře se považují za nové implementace.

Tato sada témat se zaměřuje na scénář 3 a popisuje klíčové kroky k migraci stávajícího správce front IBM MQ do prostředí kontejneru s použitím IBM MQ Operator. Vzhledem k flexibilitě a rozsáhlému použití produktu IBM MQ existuje několik volitelných kroků. Každý z nich obsahuje sekci "Musím to udělat?". Ověření, že byste měli během migrace ušetřit čas.

Musíte také zvážit, jaká data se mají migrovat:

1. Migrovat produkt IBM MQ se stejnou konfigurací, ale bez jakýchkoli existujících zpráv ve frontě.
2. Migrovat produkt IBM MQ se stejnou konfigurací a existujícími zprávami.

Typická verze pro migraci verzí může použít jeden z přístupů. V typickém správci front produktu IBM MQ v místě migrace existuje několik málo zpráv, pokud jsou nějaké uložené ve frontách, díky čemuž je volba 1 vhodná pro mnoho případů. V případě migrace na platformu kontejneru je volba 1 ještě běžnější, aby se snížila složitost migrace a umožnil tzv. blue-green deployment (modrozelené nasazení). Proto se pokyny zaměřují na tento scénář.

Cílem tohoto scénáře je vytvořit správce front v prostředí kontejneru, který odpovídá definici existujícího správce front. To umožňuje jednoduše překonfigurovat existující aplikace připojené k síti tak, aby ukazovaly na nového správce front, aniž by se změnila jakákoli jiná konfigurace nebo logika aplikace.

V rámci této migrace generujete více konfiguračních souborů, které mají být použity pro nového správce front. Chcete-li zjednodušit správu těchto souborů, měli byste vytvořit adresář a soubory vygenerovat do tohoto adresáře.

Postup

1. “Kontrola, zda jsou k dispozici požadované funkce” na stránce 80
2. “Extrakce konfigurace správce front” na stránce 80
3. Volitelné: “Volitelné: Extrakce a získání klíčů a certifikátů správce front” na stránce 81
4. Volitelné: “Volitelné: Konfigurace protokolu LDAP” na stránce 83
5. Volitelné: “Volitelné: Změna adres IP a názvů hostitelů v konfiguraci produktu IBM MQ” na stránce 90
6. “Aktualizace konfigurace správce front pro prostředí kontejnerů” na stránce 92
7. “Výběr cílové architektury vysoké dostupnosti pro produkt IBM MQ spuštěný v kontejnerech” na stránce 94
8. “Vytvoření prostředků pro správce front” na stránce 95
9. “Vytvoření nového správce front v Red Hat OpenShift” na stránce 96
10. “Ověření implementace nového kontejneru” na stránce 100

CP4I-LTS OpenShift CD Kontrola, zda jsou k dispozici požadované funkce

IBM MQ Operator nezahrnuje všechny dostupné funkce v rámci IBM MQ Advanced a vy musíte ověřit, že tyto funkce nejsou vyžadovány. Jiné funkce jsou částečně podporovány a lze je překonfigurovat tak, aby odpovídaly obsahu, který je k dispozici v kontejneru.

Než začnete

Jedná se o první krok v “Migrace IBM MQ do produktu IBM Cloud Pak for Integration” na stránce 79.

Postup

1. Ověřte, že obraz cílového kontejneru obsahuje všechny požadované funkce.

   Nejnovější informace viz “Zvolení, jak se má produkt IBM MQ používat v kontejnerech” na stránce 5.
2. IBM MQ Operator má jeden provozní port IBM MQ, známý jako listener. Máte-li více modulů listener, zjednodušte to na použití jednoho modulu listener v kontejneru. Vzhledem k tomu, že se nejedná o běžný scénář, tato úprava není podrobně dokumentována.
3. Jsou-li použity uživatelské procedury IBM MQ, proveďte jejich migraci do kontejneru, a to vrstvením v binárních souborech uživatelské procedury IBM MQ. Jedná se o scénář rozšířené migrace, a proto zde není zahrnut. Informace o postupu viz “Sestavení obrazu pomocí vlastních souborů MQSC a INI s použitím rozhraní CLI Red Hat OpenShift” na stránce 162.
4. Pokud váš systém IBM MQ zahrnuje vysokou dostupnost, zkontrolujte dostupné volby.

   Viz “Vysoká dostupnost pro IBM MQ v kontejnerech” na stránce 25.

Jak pokračovat dále

Nyní jste připraveni extrahovat konfiguraci správce front.

CP4I-LTS OpenShift CD Extrakce konfigurace správce front

Většina konfigurace je přenositelná mezi správci front. Například věci, se kterými aplikace interaguje, jako jsou definice front, témat a kanálů. Tato úloha slouží k extrakci konfigurace z existujícího správce front IBM MQ.

Než začnete

Tato úloha předpokládá, že jste zkontrolovali dostupnost požadovaných funkcí.

Postup

1. Přihlaste se k počítači s existující instalací IBM MQ.
2. Zazálohujte konfiguraci.

   Spusťte následující příkaz:

   ```
   dmpmqcfg -m QMGR_NAME > /tmp/backup.mqsc
   ```

   Poznámky k používání pro tento příkaz:

   - Tento příkaz ukládá zálohu do adresáře `tmp`. Zálohování můžete uložit do jiného umístění, ale tento scénář předpokládá adresář `tmp` pro následné příkazy.
   - *QMGR_NAME* nahraďte názvem správce front z vašeho prostředí. Pokud si nejste jisti hodnotou, spusťte příkaz **dspmq** a prohlédněte si dostupné správce front na počítači. Zde je uveden příklad výstupu příkazu **dspmq** pro správce front s názvem `qm1`:

     ```
     QMNAME(qm1)                   STATUS(Running)
     ```

Příkaz **dspmq** vyžaduje spuštění správce front IBM MQ, jinak se zobrazí následující chyba:

```
AMQ8146E: IBM MQ queue manager not available.
```

V případě potřeby spusťte správce front spuštěním následujícího příkazu:

```
strmqm QMGR_NAME
```

Jak pokračovat dále

Nyní jste připraveni extrahovat a získat klíče a certifikáty správce front.

CP4I-LTS OpenShift CD Volitelné: Extrakce a získání klíčů a certifikátů správce front

Produkt IBM MQ lze konfigurovat pomocí TLS k zašifrování provozu v rámci správce front. Tato úloha slouží k ověření, zda správce front používá TLS, k extrakci klíčů a certifikátů a ke konfiguraci TLS v migrovaném správci front.

Než začnete

Tato úloha předpokládá, že jste extrahovali konfiguraci správce front.

Informace o této úloze

Musím to udělat?

IBM MQ lze konfigurovat k zašifrování provozu v rámci správce front. Toto šifrování je dokončeno pomocí úložiště klíčů konfigurovaného ve správci front. Kanály IBM MQ potom povolí komunikaci TLS. Pokud si nejste jisti, zda je ve vašem prostředí nakonfigurována, spusťte následující příkaz k ověření:

```
grep 'SECCOMM(ALL\|SECCOMM(ANON\|SSLCIPH' backup.mqsc
```

Nejsou-li nalezeny žádné výsledky, TLS se nepoužívá. To však neznamená, že TLS by nemělo být nakonfigurováno v migrovaném správci front. Existuje řada důvodů, proč byste mohli chtít změnit toto chování:

- Přístup zabezpečení v prostředí Red Hat OpenShift by měl být vylepšen ve srovnání s předchozím prostředím.
- Potřebujete-li přístup k migrovanému správci front mimo prostředí Red Hat OpenShift, je třeba, aby TLS prošlo přes trasu Red Hat OpenShift.

Poznámka: V 9.3.2 Certifikáty správce front se stejným rozlišujícím názvem subjektu (DN) jako certifikát vydavatele (CA) nejsou podporovány. Certifikát musí mít jedinečný rozlišující název subjektu. Produkt nyní kontroluje, že DN nejsou stejná.

Postup

1. Extrahujte všechny důvěryhodné certifikáty z existujícího úložiště.

   Používáte-li se aktuálně TLS ve správci front, může mít správce front uložený počet důvěryhodných certifikátů. Je třeba je extrahovat a zkopírovat do nového správce front. Proveďte jeden z následujících volitelných kroků:

   - Chcete-li zefektivnit extrakci certifikátů, spusťte následující skript v lokálním systému:

     ```
     #!/bin/bash
     keyr=$(grep SSLKEYR $1)
     ```

```
if [ -n "${keyr}" ]; then
    keyrlocation=$(sed -n "s/^.*'\(.*\)'.*$/\1/ p" <<< ${keyr})
    mapfile -t runmqckmResult < <(runmqckm -cert -list -db ${keyrlocation}.kdb -stashed)
        cert=1
    for i in "${runmqckmResult[@]:1}"
        do
           certlabel=$(echo ${i} | xargs)
           echo Extracting certificate $certlabel to $cert.cert
       runmqckm -cert -extract -db ${keyrlocation}.kdb -label "$certlabel" -target $
{cert}.cert -stashed
       cert=$[$cert+1]
        done
fi
```

Při spuštění skriptu zadejte umístění zálohy IBM MQ jako argument a certifikáty jsou extrahovány. Pokud je například skript nazván `extractCert.sh` a záloha IBM MQ se nachází v `/tmp/backup.mqsc`, spusťte následující příkaz:

```
extractCert.sh /tmp/backup.mqsc
```

- Volitelně spusťte následující příkazy v uvedeném pořadí:

  a. Identifikujte umístění úložiště TLS:

  ```
  grep SSLKEYR /tmp/backup.mqsc
  ```

  Ukázkový výstup:

  ```
  SSLKEYR('/run/runmqserver/tls/key') +
  ```

  Kde úložiště klíčů se nachází v umístění `/run/runmqserver/tls/key.kdb`

  b. Na základě těchto informací o umístění se dotázat na úložiště klíčů, a určit tak uložené certifikáty:

  ```
  runmqckm -cert -list -db /run/runmqserver/tls/key.kdb -stashed
  ```

  Ukázkový výstup:

  ```
  Certificates in database /run/runmqserver/tls/key.kdb:
            default
            CN=cs-ca-certificate,O=cert-manager
  ```

  c. Extrahujte každý z uvedených certifikátů. Proveďte to spuštěním následujícího příkazu:

  ```
  runmqckm -cert -extract -db KEYSTORE_LOCATION -label "LABEL_NAME" -target OUTPUT_FILE
  -stashed
  ```

  V předchozích ukázkách se tento stav rovnal následujícím:

  ```
  runmqckm -cert -extract -db /run/runmqserver/tls/key.kdb -label "CN=cs-ca-
  certificate,O=cert-manager" -target /tmp/cert-manager.crt -stashed
  runmqckm -cert -extract -db /run/runmqserver/tls/key.kdb -label "default" -target /tmp/
  default.crt -stashed
  ```

2. Získejte nový klíč a certifikát pro správce front.

   Chcete-li nakonfigurovat TLS v migrovaném správci front, vygenerujte nový klíč a certifikát. To se pak použije během implementace. V mnoha organizacích to znamená kontaktovat svůj bezpečnostní tým a požádat o klíč a certifikát. V některých organizacích tato volba není k dispozici a používají se certifikáty podepsané držitelem.

Následující příklad generuje certifikát podepsaný držitelem, kde je vypršení platnosti nastaveno na 10 let:

```
openssl req \
       -newkey rsa:2048 -nodes -keyout qmgr.key \
       -subj "/CN=mq queuemanager/OU=ibm mq" \
       -x509 -days 3650 -out qmgr.crt
```

Vytvoří se dva nové soubory:

- `qmgr.key` je soukromý klíč pro správce front.
- `qmgr.crt` je veřejný certifikát

Jak pokračovat dále

Nyní jste připraveni konfigurovat LDAP.

CP4I-LTS OpenShift CD Volitelné: Konfigurace protokolu LDAP

IBM MQ Operator může být konfigurován tak, aby používal několik různých přístupů zabezpečení. Protokol LDAP je obvykle nejefektivnější pro podnikovou implementaci, a pro tento scénář migrace se používá LDAP.

Než začnete

Tato úloha předpokládá, že jste extrahovali konfiguraci správce front pro prostředí kontejneru.

Informace o této úloze

Musím to udělat?

Používáte-li již LDAP pro ověření a autorizaci, pak se nepožadují žádné změny.

Pokud si nejste jisti, zda se LDAP používá, spusťte následující příkaz:

```
connauthname="$(grep CONNAUTH backup.mqsc | cut -d "(" -f2 | cut -d ")" -f1)"; grep -A 20
AUTHINFO\($connauthname\) backup.mqsc
```

Ukázkový výstup:

```
DEFINE AUTHINFO('USE.LDAP') +
   AUTHTYPE(IDPWLDAP) +
   ADOPTCTX(YES) +
   CONNAME('ldap-service.ldap(389)') +
   CHCKCLNT(REQUIRED) +
   CLASSGRP('groupOfUniqueNames') +
   FINDGRP('uniqueMember') +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
*  LDAPPWD('********************************') +
   SHORTUSR('uid') +
   GRPFIELD('cn') +
   USRFIELD('uid') +
   AUTHORMD(SEARCHGRP) +
*  ALTDATE(2020-11-26) +
*  ALTTIME(15.44.38) +
   REPLACE
```

Ve výstupu jsou dva atributy, které jsou zvláště zajímavé:

AUTHTYPE

Pokud je tato hodnota `IDPWLDAP`, potom pro ověření používáte LDAP.

Pokud je hodnota prázdná, nebo jiná hodnota, pak LDAP není nakonfigurováno. V takovém případě zkontrolujte atribut `AUTHORMD`, abyste zjistili, zda se uživatelé LDAP používali pro autorizaci.

AUTHORMD
Pokud je tato hodnota 0S, potom pro autorizaci nepoužíváte LDAP.

Chcete-li upravit autorizaci a ověření pro použití LDAP, proveďte následující úlohy:

Postup

1. Aktualizujte zálohu produktu IBM MQ pro server LDAP.
2. Aktualizujte zálohu produktu IBM MQ pro informace o autorizaci LDAP.

Část LDAP 1: Aktualizace zálohy IBM MQ pro server LDAP

Úplný popis, jak nastavit LDAP, je mimo rozsah tohoto scénáře. Toto téma poskytuje souhrn procesu, ukázky a odkazy na další informace.

Než začnete

Tato úloha předpokládá, že jste extrahovali konfiguraci správce front pro prostředí kontejneru.

Informace o této úloze

Musím to udělat?

Používáte-li již LDAP pro ověření a autorizaci, pak se nepožadují žádné změny. Pokud si nejste jisti, zda se LDAP používá, podívejte se na téma “Volitelné: Konfigurace protokolu LDAP” na stránce 83.

Pro nastavení serveru LDAP jsou k dispozici dvě části:

1. Definujte konfiguraci LDAP.
2. Přidružte konfiguraci LDAP k definici správce front.

Další informace, které vám pomohou s touto konfigurací:

- Přehled úložiště uživatelů
- Referenční příručka k příkazu AUTHINFO

Postup

1. Definujte konfiguraci LDAP.

   Upravte soubor `backup.mqsc`, abyste definovali nový objekt **AUTHINFO** pro systém LDAP. Příklad:

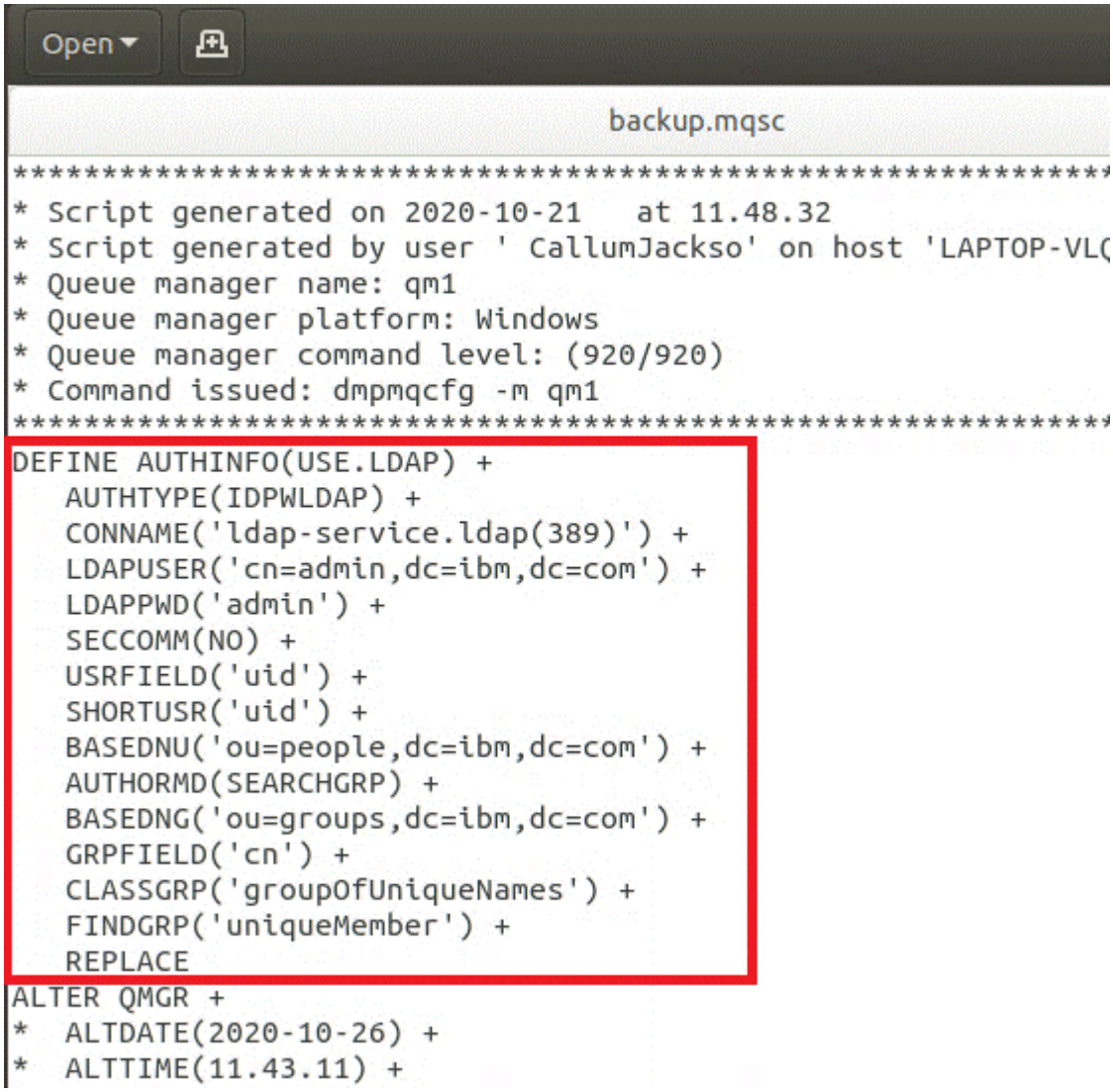
```
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
   LDAPPWD('admin') +
   SECCOMM(NO) +
   USRFIELD('uid') +
   SHORTUSR('uid') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   AUTHORMD(SEARCHGRP) +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   GRPFIELD('cn') +
   CLASSGRP('groupOfUniqueNames') +
   FINDGRP('uniqueMember')
   REPLACE
```

   kde:

   - **CONNAME** je název hostitele a port odpovídající serveru LDAP. Pokud pro odolnost existuje více adres, je možné je konfigurovat pomocí seznamu odděleného čárkami.
   - **LDAPUSER** je rozlišující název odpovídající uživateli, který produkt IBM MQ používá při připojování k LDAP, aby se dotázal na záznamy uživatelů.

- **LDAPPWD** je heslo, které odpovídá uživateli **LDAPUSER**.
- Parametr **SECCOM** určuje, zda by komunikace se serverem LDAP měla používat zabezpečení TLS. Možné hodnoty jsou:
  - YES: Používá se TLS a certifikát je prezentován serverem IBM MQ.
  - ANON: Používá se TLS bez toho, že by byl certifikát prezentován serverem IBM MQ.
  - NO: TLS se nepoužívá během připojení.
- **USRFIELD** určuje pole v záznamu LDAP, vůči němuž je prezentované jméno uživatele porovnáváno.
- **SHORTUSR** je pole v rámci záznamu LDAP, jehož délka nepřesahuje 12 znaků. Hodnota v tomto poli je deklarovaná identita, je-li ověření úspěšné.
- **BASEDNU** je základní rozlišující název, který by měl být použit pro vyhledávání LDAP.
- **BASEDNG** je základní rozlišující název pro skupiny v rámci LDAP.
- **AUTHORMD** definuje mechanizmus používaný k vyřešení členství ve skupinách pro daného uživatele. K dispozici jsou čtyři volby:
  - OS: Dotazování na operační systém pro skupiny přidružené ke krátkému názvu.
  - SEARCHGRP: Vyhledá položky skupiny v LDAP pro ověřeného uživatele.
  - SEARCHUSR: Vyhledá informace o členství ve skupinách v záznamu ověřeného uživatele.
  - SRCHGRPSN: Vyhledá položky skupiny v LDAP pro krátké jméno uživatele (definované pomocí pole SHORTUSR) pro ověřené uživatele.
- **GRPFIELD** je atribut v rámci záznamu skupiny LDAP, který odpovídá jednoduchému názvu. Je-li uveden, lze jej použít pro definování záznamů autorizace.
- **CLASSUSR** je třída objektů LDAP, která odpovídá uživateli.
- **CLASSGRP** je třída objektů LDAP, která odpovídá skupině.
- **FINDGRP** je atribut v rámci záznamu LDAP, který odpovídá členství ve skupinách.

Nová položka může být umístěna kdekoli v souboru, ale může být užitečné mít nové položky na začátku souboru:



2. Přidružte konfiguraci LDAP k definici správce front.

   Je třeba přidružit konfiguraci LDAP k definici správce front. Bezprostředně pod položkou `DEFINE AUTHINFO` je položka `ALTER QMGR`. Upravte položku CONNAUTH tak, aby odpovídala nově vytvořenému názvu AUTHINFO. Například v předchozím příkladu bylo definováno `AUTHINFO(USE.LDAP)`, což znamená, že název je `USE.LDAP`. Proto změňte `CONNAUTH('SYSTEM.DEFAULT.AUTHINFO.IDPWOS')` na `CONNAUTH('USE.LDAP')`:

Chcete-li, aby k přepnutí na LDAP došlo okamžitě, volejte příkaz `REFRESH SECURITY` přidáním řádku ihned za příkaz `ALTER QMGR`:

*backup.mqsc

```
********************************************************************
* Script generated on 2020-10-21   at 11.48.32
* Script generated by user ' CallumJackso' on host 'LAPTOP-VLQKJ5UH'
* Queue manager name: qm1
* Queue manager platform: Windows
* Queue manager command level: (920/920)
* Command issued: dmpmqcfg -m qm1
********************************************************************
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
   LDAPPWD('admin') +
   SECCOMM(NO) +
   USRFIELD('uid') +
   SHORTUSR('uid') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   AUTHORMD(SEARCHGRP) +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   GRPFIELD('cn') +
   CLASSGRP('groupOfUniqueNames') +
   FINDGRP('uniqueMember') +
   REPLACE
ALTER QMGR +
*  ALTDATE(2020-10-26) +
*  ALTTIME(11.43.11) +
   CCSID(850) +
   CERTLABL('default') +
   CLWLUSEQ(LOCAL) +
*  COMMANDQ(SYSTEM.ADMIN.COMMAND.QUEUE) +
   CONNAUTH('USE.LDAP') +
*  CRDATE(2020-10-26) +
*  CRTIME(11.43.11) +
*  QMID(qm1_2020-10-26_11.43.11) +
   SSLCRYP(' ') +
   SSLKEYR('/run/runmqserver/tls/key') +
   SUITEB(NONE) +
*  VERSION(09020000) +
   FORCE
REFRESH SECURITY
```

Jak pokračovat dále

Nyní jste připraveni aktualizovat zálohu produktu IBM MQ pro informace o autorizaci LDAP.

CP4I-LTS OpenShift CD

Část LDAP 2: Aktualizace zálohy IBM MQ pro informace o autorizaci LDAP

Produkt IBM MQ poskytuje autorizační pravidla s vysokou úrovní granularity, která řídí přístup k objektům IBM MQ. Pokud jste změnili ověření a autorizaci na LDAP, mohou být autorizační pravidla neplatná a vyžadovat aktualizaci.

Než začnete

Tato úloha předpokládá, že jste aktualizovali zálohu pro server LDAP.

Informace o této úloze

Musím to udělat?

Používáte-li již LDAP pro ověření a autorizaci, pak se nepožadují žádné změny. Pokud si nejste jisti, zda se LDAP používá, podívejte se na téma “Volitelné: Konfigurace protokolu LDAP” na stránce 83.

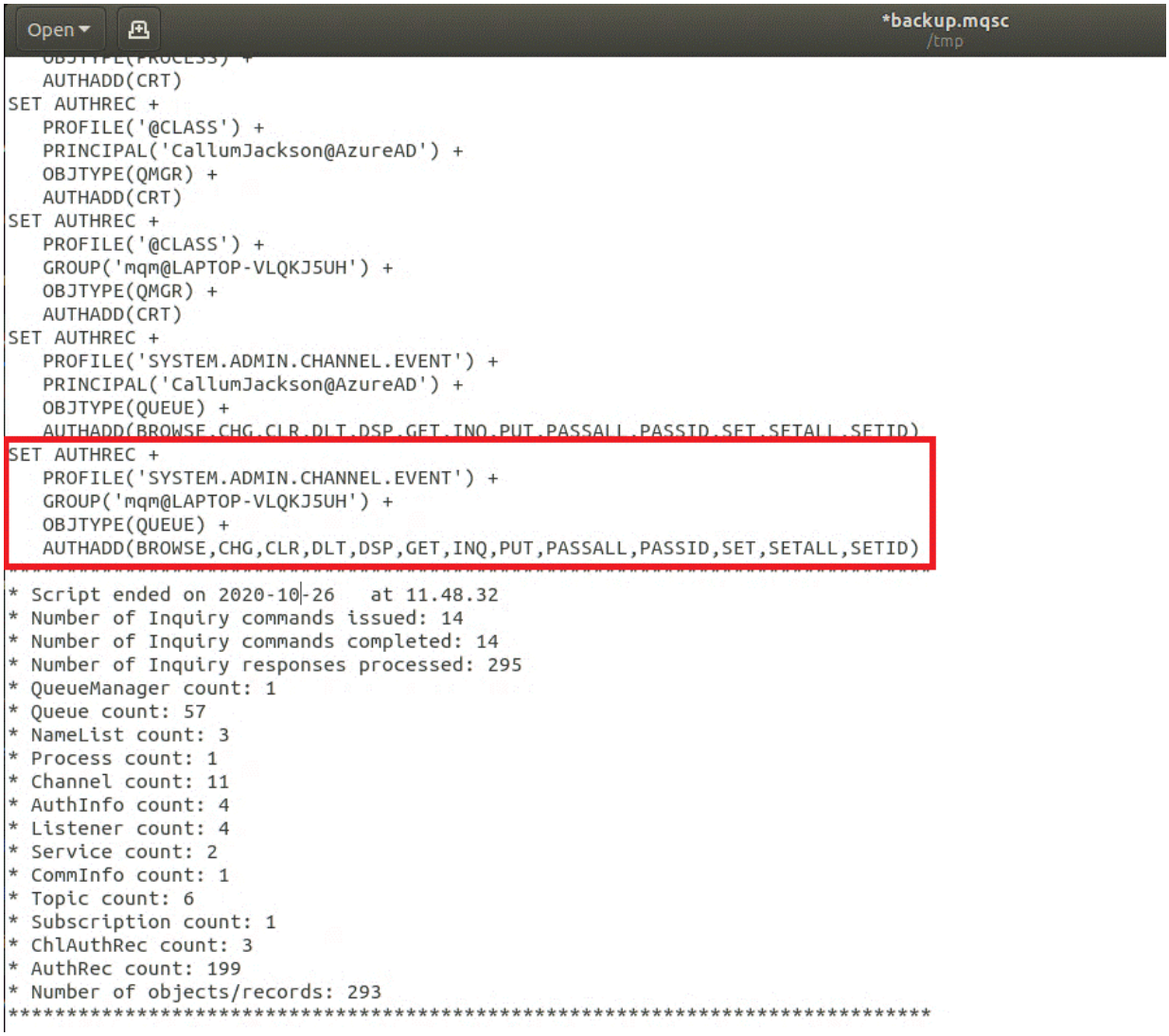
Existují dvě části pro aktualizaci informací o autorizaci LDAP:

1. Odeberte všechna existující oprávnění ze souboru.
2. Definujte nové informace o autorizaci pro LDAP.

Postup

1. Odeberte všechna existující oprávnění ze souboru.

   V souboru zálohy, v blízkosti konce souboru, byste měli vidět několik položek, které začínají položkou SET AUTHREC:



   Najděte existující položky a odstraňte je. Nejjednodušším přístupem je odebrat všechna existující pravidla SET AUTHREC a poté vytvořit nové položky založené na položkách LDAP.
2. Definujte nové informace o autorizaci pro LDAP.

V závislosti na vaší konfiguraci správce front, a počtu prostředků a skupin, může být tato činnost buď časově náročná, anebo jednoduchá. Následující příklad předpokládá, že správce front má pouze jedinou frontu s názvem Q1 a vy chcete povolit přístup skupině LDAP apps.

```
SET AUTHREC GROUP('apps') OBJTYPE(QMGR) AUTHADD(ALL)
SET AUTHREC PROFILE('Q1') GROUP('apps') OBJTYPE(QUEUE) AUTHADD(ALL)
```

První příkaz AUTHREC přidá oprávnění pro přístup ke správci front a druhý poskytuje přístup ke frontě. Je-li požadován přístup ke druhé frontě, je zapotřebí třetí příkaz AUTHREC, pokud jste se nerozhodli použít zástupné znaky k poskytnutí obecnějšího přístupu.

Zde je další příklad. Potřebuje-li skupina administrátorů (s názvem admins) úplný přístup ke správci front, přidejte následující příkazy:

```
SET AUTHREC PROFILE('*') OBJTYPE(QUEUE) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(TOPIC) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(CHANNEL) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(CLNTCONN) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(AUTHINFO) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(LISTENER) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(NAMELIST) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(PROCESS) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(SERVICE) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(QMGR) GROUP('admins') AUTHADD(ALL)
```

Jak pokračovat dále

Nyní jste připraveni změnit adresy IP a názvy hostitelů v konfiguraci IBM MQ.

CP4I-LTS OpenShift CD Volitelné: Změna adres IP a názvů hostitelů v konfiguraci produktu IBM MQ

Je možné, že konfigurace produktu IBM MQ má zadané adresy IP a názvy hostitelů. V některých situacích mohou zůstat, zatímco v jiných situacích je třeba je aktualizovat.

Než začnete

Tato úloha předpokládá, že máte nakonfigurovaný protokol LDAP.

Informace o této úloze

Musím to udělat?

Nejprve určete, zda jsou k dispozici nějaké adresy IP nebo názvy hostitelů, kromě konfigurace LDAP definované v předchozí sekci. Chcete-li to provést, spusťte následující příkaz:

```
grep 'CONNAME\|LOCLADDR\|IPADDRV' -B 3  backup.mqsc
```

Ukázkový výstup:

```
*****************************************************
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
--
DEFINE AUTHINFO('SYSTEM.DEFAULT.AUTHINFO.IDPWLDAP') +
   AUTHTYPE(IDPWLDAP) +
   ADOPTCTX(YES) +
   CONNAME(' ') +
--
   REPLACE
DEFINE AUTHINFO('SYSTEM.DEFAULT.AUTHINFO.CRLLDAP') +
```

```
   AUTHTYPE(CRLLDAP) +
   CONNAME(' ') +
```

V tomto příkladu hledání vrátí tři výsledky. Jeden výsledek odpovídá dříve definované konfiguraci LDAP. To může být ignorováno, protože název hostitele serveru LDAP zůstává stejný. Další dva výsledky jsou prázdné položky připojení, takže je lze také ignorovat. Nemáte-li žádné další položky, můžete zbývající část tématu přeskočit.

Postup

1. Seznamte se s vrácenými položkami.

   Produkt IBM MQ může zahrnovat adresy IP, názvy hostitelů a porty v rámci mnoha aspektů konfigurace. Můžeme je klasifikovat do dvou kategorií:

   a. **Umístění tohoto správce front**: Informace o umístění, které tento správce front používá nebo publikuje, které mohou ostatní správci front nebo aplikace v rámci sítě IBM MQ používat pro konektivitu.

   b. **Umístění závislostí správce front**: Umístění jiných správců front nebo systémů, které tento správce front potřebuje znát.

   Protože se tento scénář zaměřuje pouze na změny provedené v této konfiguraci správce front, zpracujeme pouze aktualizace konfigurace pro kategorii (a). Je-li však toto umístění správce front odkazováno jinými správci front nebo aplikacemi, může jejich konfigurace vyžadovat aktualizaci, aby odpovídala novému umístění správce front.

   Existují dva klíčové objekty, které mohou obsahovat informace, které je třeba aktualizovat:

   - Moduly listener: Představují síťovou adresu, na které produkt IBM MQ naslouchá.
   - Kanál RECEIVER CLUSTER: Pokud je správce front částí klastru IBM MQ, pak tento objekt existuje. Určuje síťovou adresu, ke které se mohou připojit další správci front.

2. V původním výstupu příkazu `grep 'CONNAME\|LOCLADDR\|IPADDRV' -B 3 backup.mqsc` identifikujte, zda jsou definovány kanály CLUSTER RECEIVER. Pokud tomu tak je, aktualizujte adresy IP.

   Chcete-li identifikovat, zda jsou nadefinovány kanály CLUSTER RECEIVER, vyhledejte v původním výstupu všechny položky s CHLTYPE (CLUSRCVR):

   ```
   DEFINE CHANNEL(ANY_NAME) +
      CHLTYPE(CLUSRCVR) +
   ```

   Pokud položky existují, aktualizujte CONNAME pomocí IBM MQ Red Hat OpenShift Route. Tato hodnota je založena na prostředí Red Hat OpenShift a používá předvídatelnou syntaxi:

   ```
   queue_manager_resource_name-ibm-mq-qm-openshift_project_name.openshift_app_route_hostname
   ```

   Je-li například implementace správce front pojmenována `qm1` v rámci oboru názvů `cp4i` a *openshift_app_route_hostname* je `apps.callumj.icp4i.com`, potom je adresa URL trasy tato:

   ```
   qm1-ibm-mq-qm-cp4i.apps.callumj.icp4i.com
   ```

   Číslo portu pro trasu je obvykle 443. Pokud vám administrátor Red Hat OpenShift neřekne jinak, jedná se obvykle o správnou hodnotu. Pomocí těchto informací aktualizujte pole CONNAME. Příklad:

   ```
   CONNAME('qm1-ibm-mq-qm-cp4i.apps.callumj.icp4i.com(443)')
   ```

   V původním výstupu příkazu `grep 'CONNAME\|LOCLADDR\|IPADDRV' -B 3 backup.mqsc` ověřte, zda existují nějaké položky pro LOCLADDR nebo IPADDRV. Pokud ano, odstraňte je. Nejsou relevantní v prostředí kontejnerů.

Jak pokračovat dále

Nyní jste připraveni aktualizovat konfiguraci správce front pro prostředí kontejnerů.

Aktualizace konfigurace správce front pro prostředí kontejnerů

Při spuštění v kontejneru jsou určité aspekty konfigurace definovány kontejnerem a mohou být v konfliktu s exportovanou konfigurací.

Než začnete

Tato úloha předpokládá, že jste změnili konfiguraci IBM MQ adres IP a názvů hostitelů.

Informace o této úloze

Následující aspekty konfigurace jsou definovány kontejnerem:

- Definice modulu listener (které odpovídají vystaveným portům).
- Umístění jakéhokoli potenciálního úložiště TLS.

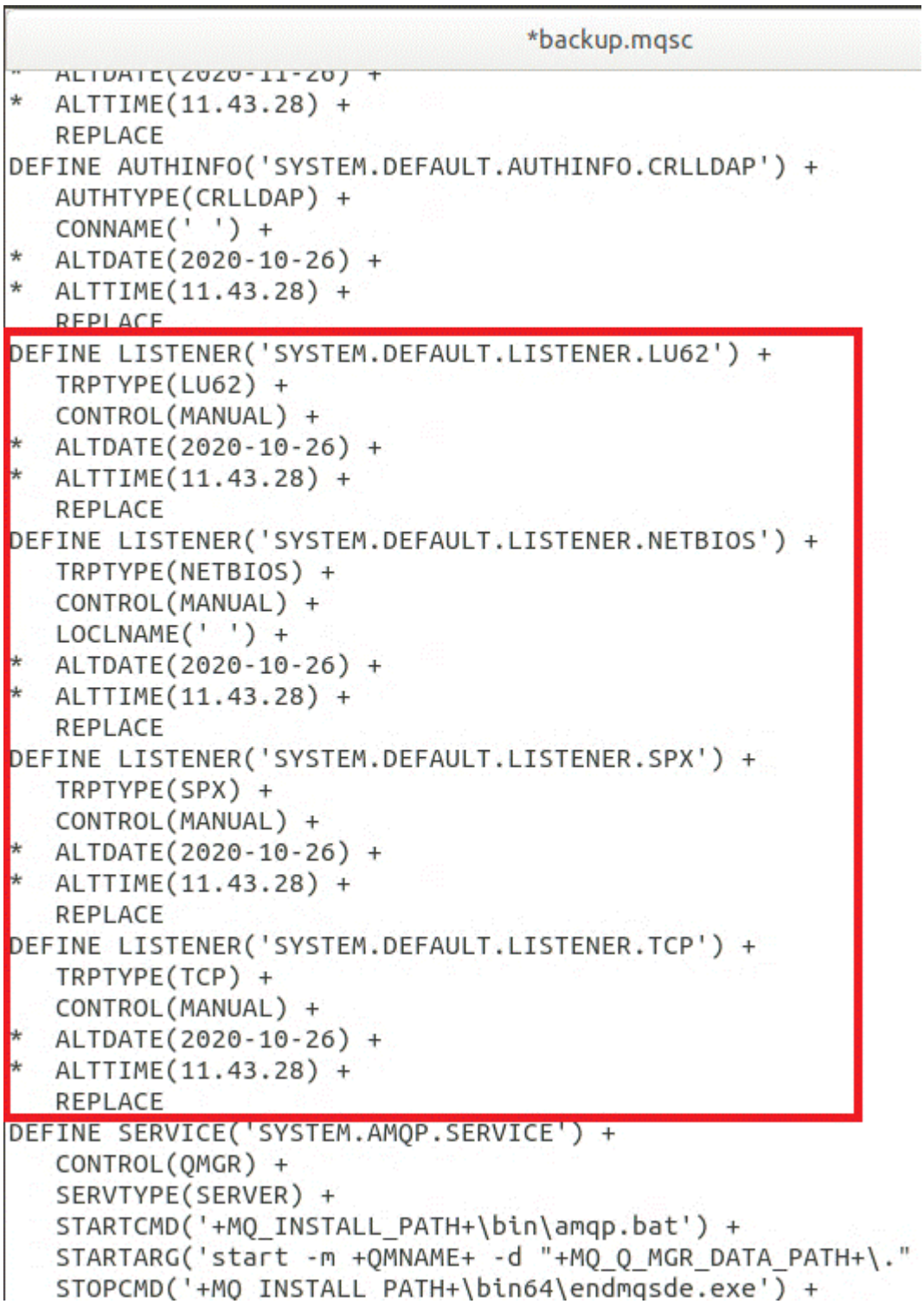
Proto je nutné aktualizovat vyexportovanou konfiguraci:

1. Odeberte všechny definice modulu listener.
2. Definujte umístění úložiště klíčů TLS.

Postup

1. Odeberte všechny definice modulu listener.

   V záložní konfiguraci vyhledejte `DEFINE LISTENER`. To by mělo být mezi definicemi `AUTHINFO` a `SERVICE`. Zvýrazněte oblast a odstraňte ji.



2. Definujte umístění úložiště klíčů TLS.

   Záloha správce front obsahuje konfiguraci TLS pro původní prostředí. To se liší od prostředí kontejneru, a proto je zapotřebí několik aktualizací:

   - Změňte položku **CERTLABL** na `default`.
   - Změňte umístění úložiště klíčů TLS (**SSLKEYR**) na: `/run/runmqserver/tls/key`.

   Chcete-li najít umístění atributu **SSLKEYR** v souboru, vyhledejte **SSLKEYR**. Obvykle je nalezena pouze jedna položka. Je-li nalezeno více položek, zkontrolujte, zda upravujete objekt **QMGR**, jak je znázorněno na následujícím obrázku:

*backup.mqsc

```
************************************************************************
* Script generated on 2020-10-21   at 11.48.32
* Script generated by user ' CallumJackso' on host 'LAPTOP-VLQKJ5UH'
* Queue manager name: qm1
* Queue manager platform: Windows
* Queue manager command level: (920/920)
* Command issued: dmpmqcfg -m qm1
************************************************************************
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
   LDAPPWD('admin') +
   SECCOMM(NO) +
   USRFIELD('uid') +
   SHORTUSR('uid') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   AUTHORMD(SEARCHGRP) +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   GRPFIELD('cn') +
   CLASSGRP('groupOfUniqueNames') +
   FINDGRP('uniqueMember') +
   REPLACE
ALTER QMGR +
*  ALTDATE(2020-10-26) +
*  ALTTIME(11.43.11) +
   CCSID(850) +
   CERTLABL('default') +
   CLWLUSEQ(LOCAL) +
*  COMMANDQ(SYSTEM.ADMIN.COMMAND.QUEUE) +
   CONNAUTH('USE.LDAP') +
*  CRDATE(2020-10-26) +
*  CRTIME(11.43.11) +
*  QMID(qm1_2020-10-26_11.43.11) +
   SSLCRYP(' ') +
   SSLKEYR('/run/runmqserver/tls/key') +
   SUITEB(NONE) +
*  VERSION(09020000) +
   FORCE
REFRESH SECURITY
```

Jak pokračovat dále

Nyní jste připraveni vybrat cílovou architekturu pro produkt IBM MQ spuštěný v kontejnerech.

CP4I-LTS OpenShift CD Výběr cílové architektury vysoké dostupnosti pro produkt IBM MQ spuštěný v kontejnerech

Vyberte si mezi jednou instancí (jediný pod Kubernetes) a více instancemi (dva pody), abyste splnili požadavky na vysokou dostupnost.

Než začnete

Tato úloha předpokládá, že jste aktualizovali konfiguraci správce front pro prostředí kontejneru.

Informace o této úloze

IBM MQ Operator poskytuje dvě volby vysoké dostupnosti:

- **Jediná instance**: Jeden kontejner (Pod) je spuštěn a Red Hat OpenShift je zodpovědný za restartování v případě selhání. Vzhledem k charakteristice stavové sady v rámci Kubernetes existuje několik situací, kdy může toto překonání selhání trvat delší dobu, nebo vyžadovat provedení administrativní akce.
- **Více instancí**: Dva kontejnery (každý v odděleném podu) jsou spuštěny, jeden v aktivním režimu a druhý v pohotovostním režimu. Tato topologie umožňuje mnohem rychlejší překonání selhání. Vyžaduje systém souborů RWX (Read Write Many) vyhovující požadavkům produktu IBM MQ.

V této úloze vyberete pouze cílovou architekturu HA. Kroky pro konfiguraci zvolené architektury jsou popsány v následující úloze v tomto scénáři (“Vytvoření nového správce front v Red Hat OpenShift” na stránce 96).

Postup

1. Zkontrolujte dvě volby.

   Úplný popis těchto dvou voleb viz “Vysoká dostupnost pro IBM MQ v kontejnerech” na stránce 25.
2. Vyberte cílovou architekturu HA.

   Pokud si nejste jisti tím, jakou volbu vybrat, začněte volbou **Jedna instance** a ověřte, zda tato volba splňuje vaše požadavky na vysokou dostupnost.

Jak pokračovat dále

Nyní jste připraveni vytvořit konfiguraci správce front.

CP4I-LTS OpenShift CD Vytvoření prostředků pro správce front

Naimportujte konfiguraci produktu IBM MQ a certifikáty a klíče TLS do prostředí Red Hat OpenShift.

Než začnete

Tato úloha předpokládá, že jste vybrali cílovou architekturu pro produkt IBM MQ spuštěný v kontejnerech.

Informace o této úloze

V předchozích sekcích jste extrahovali, aktualizovali a definovali dva prostředky:

- Konfigurace produktu IBM MQ
- Certifikáty a klíče TLS

Tyto prostředky je třeba importovat do prostředí Red Hat OpenShift před implementací správce front.

Postup

1. Importujte konfiguraci IBM MQ do produktu Red Hat OpenShift.

   Následující pokyny předpokládají, že máte konfiguraci produktu IBM MQ v aktuálním adresáři, v souboru s názvem `backup.mqsc`. Jinak je nutné upravit název souboru na základě vašeho prostředí.

   a) Přihlaste se do klastru pomocí `oc login`.

   b) Načtěte konfiguraci produktu IBM MQ do `configmap`.

Spusťte následující příkaz:

```
oc create configmap my-mqsc-migrated --from-file=backup.mqsc
```

c) Ověřte, zda byl soubor úspěšně načten.

Spusťte následující příkaz:

```
oc describe configmap my-mqsc-migrated
```

2. Naimportujte prostředky TLS produktu IBM MQ.

Jak je uvedeno v tématu “Volitelné: Extrakce a získání klíčů a certifikátů správce front” na stránce 81, TLS může být vyžadováno pro implementaci správce front. Pokud tomu tak je, měli byste již mít počet souborů ukončených pomocí `.crt` a `.key`. Musíte je přidat do tajných klíčů Kubernetes pro správce front, na který se odkazuje v době implementace.

Máte-li například klíč a certifikát pro správce front, mohou být volány:

- `qmgr.crt`
- `qmgr.key`

Chcete-li tyto soubory naimportovat, spusťte následující příkaz:

```
oc create secret tls my-tls-migration --cert=qmgr.crt --key=qmgr.key
```

Kubernetes poskytuje tento užitečný obslužný program, když importujete odpovídající veřejný a soukromý klíč. Máte-li k dispozici další certifikáty, které chcete přidat, například do úložiště údajů o důvěryhodnosti správce front, spusťte následující příkaz:

```
oc create secret generic my-extra-tls-migration --from-file=comma_separated_list_of_files
```

Pokud jsou například soubory, které mají být importovány, `trust1.crt`, `trust2.crt` a `trust3.crt`, příkaz je následující:

```
oc create secret generic my-extra-tls-migration --from-file=trust1.crt,trust2.crt,trust3.crt
```

Jak pokračovat dále

Nyní jste připraveni vytvořit nového správce front v Red Hat OpenShift.

CP4I-LTS OpenShift CD Vytvoření nového správce front v Red Hat OpenShift

Implementujte buď pouze jednu instanci, nebo správce front s více instancemi v Red Hat OpenShift.

Než začnete

Tato úloha předpokládá, že máte vytvořené prostředky správce front a nainstalován IBM MQ Operator do Red Hat OpenShift.

Informace o této úloze

Jak je uvedeno v části “Výběr cílové architektury vysoké dostupnosti pro produkt IBM MQ spuštěný v kontejnerech” na stránce 94, existují dvě možné topologie implementace. V tomto tématu jsou k dispozici dvě různé šablony:

- Implementujte správce front s jednou instancí.
- Implementujte správce front s více instancemi.

Důležité: Na základě vaší preferované topologie proveďte pouze jednu z těchto dvou šablon.

Procedura

- Implementujte správce front s jednou instancí.

  Migrovaný správce front je implementován do Red Hat OpenShift pomocí souboru YAML. Zde je ukázka, která je založena na názvech použitých v předchozích tématech:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm1
spec:
  version: 9.3.5.1-r2
  license:
    accept: true
    license: L-VTPK-22YZPK
    use: "Production"
  pki:
    keys:
    - name: default
      secret:
        secretName: my-tls-migration
        items:
          - tls.key
          - tls.crt
  web:
    enabled: true
  queueManager:
    name: QM1
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

  V závislosti na krocích, které jste provedli, může být nutné předchozí YAML upravit. Chcete-li s tímto pomoci, je zde vysvětlení tohoto YAML:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm1
```

  Definuje objekt Kubernetes, typ a název. Jediné pole vyžadující přizpůsobení je pole `name`.

```
 spec:
  version: 9.3.5.1-r2
  license:
    accept: true
    license: L-VTPK-22YZPK
    use: "Production"
```

  This corresponds to the version and license information for the deployment. If you need to customize this, use the information provided in “Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 179.

```
  pki:
    keys:
    - name: default
      secret:
        secretName: my-tls-migration
        items:
          - tls.key
          - tls.crt
```

  Aby mohl být správce front konfigurován tak, aby používal TLS, musí odkazovat na příslušné certifikáty a klíče. Pole `secretName` odkazuje na tajný údaj Kubernetes vytvořený v sekci Importovat prostředky TLS produktu IBM MQ a seznam položek (`tls.key` a `tls.crt`) jsou standardní názvy, které produkt Kubernetes přiřazuje při použití syntaxe `oc create secret tls`. Máte-li další certifikáty, které

chcete přidat do úložiště údajů o důvěryhodnosti, můžete tyto certifikáty přidat podobným způsobem, ale tyto položky představují odpovídající názvy souborů použité během importu. K vytvoření certifikátů úložiště údajů o důvěryhodnosti lze například použít následující kód:

```
oc create secret generic my-extra-tls-migration --from-file=trust1.crt,trust2.crt,trust3.crt
```

```
  pki:
    trust:
    - name: default
      secret:
        secretName: my-extra-tls-migration
        items:
          - trust1.crt
          - trust2.crt
          - trust3.crt
```

Důležité: Není-li zabezpečení TLS vyžadováno, odstraňte sekci TLS v YAML.

```
  web:
    enabled: true
```

To umožňuje webovou konzolu pro implementaci

```
  queueManager:
    name: QM1
```

Definuje název správce front jako QM1. Správce front je upraven na základě vašich požadavků, například jaký byl původní název správce front.

```
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

Předchozí kód se stáhne do konfigurace správce front, která byla naimportována v sekci Import konfigurace IBM MQ. Pokud jste použili jiné názvy, je třeba upravit `my-mqsc-migrated` a `backup.mqsc`.

Všimněte si, že ukázka YAML předpokládá, že výchozí paměťová třída pro prostředí Red Hat OpenShift je definována jako třída úložiště RWX nebo RWO. Není-li ve vašem prostředí definováno výchozí nastavení, je nutné určit paměťovou třídu, která má být použita. Toto můžete provést rozšířením YAML takto:

```
  queueManager:
    name: QM1
    storage:
      defaultClass: my_storage_class
      queueManager:
        type: persistent-claim
```

Přidejte zvýrazněný text s přizpůsobeným atributem třídy, aby odpovídal vašemu prostředí. Chcete-li zjistit názvy paměťových tříd ve svém prostředí, spusťte následující příkaz:

```
oc get storageclass
```

Zde je příklad výstupu vráceného tímto příkazem:

```
NAME          PROVISIONER             RECLAIMPOLICY
aws-efs       openshift.org/aws-efs   Delete
gp2 (default) kubernetes.io/aws-ebs   Delete
```

Následující kód ukazuje, jak odkazovat na konfiguraci IBM MQ, která byla naimportována v sekci Import konfigurace produktu IBM MQ. Pokud jste použili jiné názvy, je třeba upravit `my-mqsc-migrated` a `backup.mqsc`.

```
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

Implementovali jste správce front s jednou instancí. Tím je dokončena šablona. Nyní jste připraveni ověřit novou implementace kontejneru.

- Implementujte správce front s více instancemi.

  Migrovaný správce front je implementován do Red Hat OpenShift pomocí souboru YAML. Následující ukázka je založena na názvech použitých v předchozích sekcích.

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm1mi
spec:
  version: 9.3.5.1-r2
  license:
    accept: true
    license: L-VTPK-22YZPK
    use: "Production"
  pki:
    keys:
    - name: default
      secret:
        secretName: my-tls-migration
        items:
          - tls.key
          - tls.crt
  web:
    enabled: true
  queueManager:
    name: QM1
    availability: MultiInstance
    storage:
      defaultClass: aws-efs
      persistedData:
        enabled: true
      queueManager:
        enabled: true
      recoveryLogs:
        enabled: true
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

Zde je vysvětlení tohoto YAML. Většina konfigurace má stejný přístup jako implementace správce front s jednou instancí, proto jsou zde vysvětleny pouze aspekty dostupnosti správce front a úložiště.

```
queueManager:
    name: QM1
    availability: MultiInstance
```

Určuje název správce front jako `QM1` a nastavuje implementaci `MultiInstance` místo výchozí jediné instance.

```
    storage:
      defaultClass: aws-efs
      persistedData:
        enabled: true
      queueManager:
        enabled: true
```

```
      recoveryLogs:
        enabled: true
```

Správce front s více instancemi produktu IBM MQ závisí na úložišti RWX. Standardně je správce front implementován v režimu jedné instance, a proto jsou při přechodu na režim více instancí zapotřebí další volby úložiště. V předchozí ukázce YAML jsou definovány tři trvalé svazky úložišť a trvalá třída svazku. Tato trvalá třída svazku musí být paměťová třída RWX. Pokud si nejste jisti názvy paměťových tříd ve vašem prostředí, můžete spustit následující příkaz a zjistit je:

```
oc get storageclass
```

Zde je příklad výstupu vráceného tímto příkazem:

```
NAME          PROVISIONER             RECLAIMPOLICY
aws-efs       openshift.org/aws-efs   Delete
gp2 (default) kubernetes.io/aws-ebs   Delete
```

Následující kód ukazuje, jak odkazovat na konfiguraci IBM MQ, která byla naimportována v sekci Import konfigurace produktu IBM MQ. Pokud jste použili jiné názvy, je třeba upravit `my-mqsc-migrated` a `backup.mqsc`.

```
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

Implementovali jste správce front s více instancemi. Tím je dokončena šablona. Nyní jste připraveni ověřit novou implementace kontejneru.

CP4I-LTS OpenShift CD Ověření implementace nového kontejneru

Nyní, když je produkt IBM MQ implementován v Red Hat OpenShift, můžete ověřit prostředí pomocí ukázek produktu IBM MQ.

Než začnete

Tato úloha předpokládá, že jste vytvořili nového správce front v Red Hat OpenShift.

Důležité: Tato úloha předpokládá, že TLS není v daném správci front povoleno.

Informace o této úloze

V této úloze spustíte ukázky produktu IBM MQ z kontejneru správce front převedeného migrací. Je však možné, že budete chtít používat vlastní aplikace spuštěné v jiném prostředí.

Potřebujete tyto informace:

- Jméno uživatele LDAP
- Heslo LDAP
- IBM MQ - Název kanálu
- Název fronty

Tento vzorový kód používá následující nastavení. Všimněte si, že vaše nastavení se bude lišit.

- Jméno uživatele LDAP: mqapp
- Heslo LDAP: mqapp
- Název kanálu produktu IBM MQ: DEV.APP.SVRCONN
- Název fronty: Q1

Postup

1. Exec do spuštěného kontejneru IBM MQ.

   Zadejte následující příkaz:

   ```
   oc exec -it qm1-ibm-mq-0 /bin/bash
   ```

   Kde `qm1-ibm-mq-0` je pod, který jsme implementovali v “Vytvoření nového správce front v Red Hat OpenShift” na stránce 96. Pokud jste implementaci nazvali něčím jiným, upravte tuto hodnotu.
2. Odešlete zprávu.

   Spusťte následující příkazy:

   ```
   cd /opt/mqm/samp/bin
   export IBM MQSAMP_USER_ID=mqapp
   export IBM MQSERVER=DEV.APP.SVRCONN/TCP/'localhost(1414)'
   ./amqsputc Q1 QM1
   ```

   Zobrazí se výzva k zadání hesla a poté můžete odeslat zprávu.
3. Ověřte, zda byla zpráva úspěšně přijata.

   Spusťte ukázku GET:

   ```
   ./amqsgetc Q1 QM1
   ```

Výsledky

Dokončili jste “Migrace IBM MQ do produktu IBM Cloud Pak for Integration” na stránce 79.

Jak pokračovat dále

Použijte následující informace, které vám pomohou se složitějšími scénáři migrace:

Migrace zpráv ve frontě
: Chcete-li migrovat existující zprávy ve frontě, postupujte podle pokynů v následujícím tématu pro export a import zpráv po zavedení nového správce front: Použití obslužného programu dmpmqmsg mezi dvěma systémy.

Připojení k produktu IBM MQ mimo prostředí Red Hat OpenShift
: Implementovaný správce front může být vystaven klientům IBM MQ a správcům front mimo prostředí Red Hat OpenShift. Proces závisí na verzi produktu IBM MQ, která se připojuje k prostředí Red Hat OpenShift. Viz téma “Konfigurace trasy pro připojení ke správci front mimo klastr Red Hat OpenShift” na stránce 152.

OpenShift CP4I Instalace produktu IBM MQ Operator

Produkt IBM MQ Operator lze nainstalovat do systému Red Hat OpenShift pomocí konzoly OpenShift nebo rozhraní příkazového řádku (CLI).

Než začnete

Chcete-li zajistit, aby instalace probíhala co nejplynuleji, před zahájením instalace se ujistěte, že jste porozuměli všem předpokladům a požadavkům. Viz “Plánování pro IBM MQ v kontejnerech” na stránce 5.

Důležité: V 9.3.4 Před instalací produktu IBM MQ Operatorsi prostudujte pokyny týkající se strukturování implementace .

Informace o této úloze

Následující kroky představují typický tok úloh pro instalaci produktu IBM MQ Operator:

1. Instalovat Red Hat OpenShift Container Platform.
2. Konfigurovat úložiště.
3. Zrcadlové obrazy (pouze vzduchová mezera).
4. Přidejte katalog operátorů IBM a připravte klastr.
5. Nainstalujte zařízení IBM MQ Operator.
6. Vytvořit tajný klíč nároku (pouze instalace online).
7. Volitelné: Nainstalujte IBM Cloud Pak for Integration (CP4I) a jeho závislosti.
8. Implementujte License Service.
9. Implementovat správce front.

Postup

1. Nainstalujte produkt Red Hat OpenShift Container Platform.

   Podrobné kroky k instalaci produktu OpenShiftnaleznete v tématu Instalace softwaru Red Hat 4.6 nebo novější.

   Důležité: Ujistěte se, že instalujete podporovanou verzi produktu OpenShift Container Platform. Chcete-li například použít produkt IBM MQ Operator 2.0 nebo novější, musíte nainstalovat produkt OpenShift Container Platform 4.12 nebo novější. Všimněte si také, že jsou podporována pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí verze se sudým číslem, například 4.14 a 4.16. Další informace viz IBM Cloud Pak a Red Hat OpenShift Container Platform kompatibilita.

   Pro všechny kroky, které používají rozhraní příkazového řádku Red Hat OpenShift Container Platform , musíte být přihlášeni ke svému klastru OpenShift pomocí `oc login`. Chcete-li nainstalovat rozhraní CLI, prohlédněte si téma Začínáme s rozhraním OpenShift CLI.

   Po instalaci produktu OpenShiftmůžete ověřit a získat přístup k softwaru kontejneru pomocí klíče nároku IBM , který vytvoříte v části Vytvořit tajný klíč nároku.
2. Konfigurovat úložiště.

   Musíte nadefinovat paměťové třídy v produktu Red Hat OpenShift Container Platform a nastavit konfiguraci úložiště tak, aby splňovala vaše požadavky na velikost.

   Důležité: IBM MQ správci front s jednou instancí a nativním HA mohou používat režim přístupu RWO, zatímco správci front s více instancemi vyžadují RWX, jak je popsáno v tématu “Aspekty úložiště pro IBM MQ Operator” na stránce 20. IBM MQ správci front s více instancemi vyžadují určité charakteristiky systému souborů, které lze ověřit pomocí pokynů pro Testování sdíleného systému souborů pro produkt IBM MQ.

   Seznam známých vyhovujících a nevyhovujících systémů souborů a poznámky k dalším omezením naleznete v Prohlášení o testování pro systémy souborů IBM MQ.

   Doporučené poskytovatele úložiště lze nalézt na stránce CP4I Aspekty úložiště .
3. V 9.3.4

   Zrcadlové obrazy (pouze vzduchová mezera).

   Pokud se váš klastr nachází v omezeném síťovém prostředí (s omezením), musíte zrcadlit obrazy IBM MQ . V závislosti na konfiguraci může být také nutné zrcadlit některé další komponenty. Přečtěte si následující informace a zrcadlete obrazy podle potřeby.

   - Musíte zrcadlit obrazy IBM MQ . Použijte následující hodnoty:

     ```
     export OPERATOR_PACKAGE_NAME=ibm-mq
     export OPERATOR_VERSION=3.1.3
     ```

- Pokud hodláte implementovat alespoň jednoho správce front, u kterého platí **všechny** následující příkazy, musíte také zrcadlit některé další nezbytné komponenty:
  - Používáte verzi IBM MQ 9.3.4 nebo novější.
  - Používáte licenci CP4I .
  - Parametr IBM MQ Console je povolen.
  - Používáte službu IBM Cloud Pak for Integration Keycloak pro ověření a autorizaci jednotného přihlášení IBM MQ Console (SSO) (předvolba).

  Pokud jsou předchozí příkazy pravdivé, pak je jednotné přihlášení poskytováno produktem Keycloak a musíte zrcadlit každou z následujících komponent:
  - IBM Cloud Pak foundational services
  - Certificate Manager. Pokud jste nainstalovali verzi operátora IBM Cloud Pak foundational services před verzí 4.4, musíte zrcadlit Certificate Manager.[6]
  - IBM Cloud Pak for Integration
  - Keycloak (Red Hat OpenShift operátor)

  Chcete-li vytvořit zrcadlové obrazy, prohlédněte si téma Zrcadlení obrazů pro klastr s omezením vzduchu.
4. Přidejte zdroj katalogu IBM MQ Operator .

   Přidejte zdroj katalogu, který zpřístupní operátory pro váš klastr. Viz “Přidání zdroje katalogu IBM MQ Operator” na stránce 104.
5. Nainstalujte IBM MQ Operator.

   Vyberte jednu z následujících dvou voleb (použijte konzolu nebo rozhraní CLI):
   - Volba 1: Instalovat produkt IBM MQ Operator pomocí OpenShift konzoly.
   - Volba 2: Instalovat produkt IBM MQ Operator pomocí rozhraní OpenShift CLI.
6. Vytvořte tajný klíč nároku (pouze instalace online).

   Produkt IBM MQ Operator implementuje obrazy správce front stažené z registru kontejnerů, který provádí kontrolu nároku na licenci. Tato kontrola vyžaduje klíč oprávnění, který je uložen v tajném údaji stažení `docker-registry`. Pokud ještě nemáte klíč oprávnění v oboru názvů, do kterého budete instalovat správce front, postupujte podle těchto pokynů, abyste získali klíč oprávnění a vytvořili tajný klíč stažení.

   Poznámka: Klíč oprávnění není vyžadován, pokud budou implementováni pouze správci front IBM MQ Advanced for Developers (bez záruky).

   Tajný klíč nároku můžete vytvořit buď pomocí konzoly OpenShift , nebo pomocí rozhraní příkazového řádku. Následující příklad používá rozhraní CLI:

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

   c. V rozhraní CLI produktu OpenShift spusťte následující příkaz, abyste vytvořili tajný klíč stažení obrazu s názvem `ibm-entitlement-key`.

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

[6] Od verze 4.4 IBM Cloud Pak foundational services již toto zrcadlení není vyžadováno.

Kde < *entitlement-key*> je klíč nároku, který jste zkopírovali v kroku b, < *user-email*> je ID IBM přidružené k oprávněnému softwaru a < *namespace*> je obor názvů, do kterého jste nainstalovali produkt IBM MQ Operator .

7. Volitelné: Nainstalujte produkt CP4I a jeho závislosti.

   Při implementaci alespoň jednoho správce front, ve kterém platí **všechny** následující příkazy, je třeba provést několik dalších nezbytných komponent:

   - Používáte verzi IBM MQ 9.3.4 nebo novější.
   - Používáte licenci CP4I .
   - Parametr IBM MQ Console je povolen.
   - Používáte službu CP4I Keycloak pro ověření a autorizaci jednotného přihlášení IBM MQ Console (SSO) (předvolba).

   Pokud jsou všechny předchozí příkazy pravdivé, pak je jednotné přihlášení poskytováno produktem Keycloak a musíte provést následující další kroky:

   - Nainstalujte operátor IBM Cloud Pak foundational services ve stejném režimu instalace jako operátor CP4I . Podporované verze viz Verze kanálu operátora pro toto vydání .
   - Pokud jste nainstalovali verzi operátoru IBM Cloud Pak foundational services před verzí 4.4, nainstalujte Operátor správce certifikátů pro produkt Red Hat OpenShift Container Platform.[7]
   - Nainstalujte CP4I Operátor.
   - Volitelné: Implementujte uživatelské rozhraní platformy.

     a. Vytvořte obor názvů `ibm-common-services` . Když se přihlásíte do klastru OpenShift pomocí rozhraní příkazového řádku, spusťte tento příkaz:

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

     b. Implementujte uživatelské rozhraní platformy.

8. Implementujte License Service.

   Toto je nezbytné pro monitorování využití licencí správců front. Postupujte podle pokynů v části Implementace License Service.

9. Implementujte správce front.

   Pokyny k implementaci ukázkového "rychlého spuštění" správce front viz “Implementace správce front do klastru Red Hat OpenShift Container Platform” na stránce 114.

Související úlohy

“Odinstalace produktu IBM MQ Operator” na stránce 117
Konzolu Red Hat OpenShift nebo rozhraní příkazového řádku můžete použít k odinstalaci produktu IBM MQ Operator z adresáře Red Hat OpenShift.

Související odkazy

“Instalace produktu IBM MQ Operator 2.x v prostředí vzduchové mezery” na stránce 108
Tento výukový program vás provede instalací produktu IBM MQ Operator 2.x do klastru Red Hat OpenShift , který nemá připojení k Internetu. Produkt IBM MQ Operator můžete nainstalovat v prostředí vzduchové mezery pomocí přenosného úložného zařízení nebo pomocí počítače typu bastion.

OpenShift CP4I Přidání zdroje katalogu IBM MQ Operator

Přidáním zdroje katalogu do klastru OpenShift přidáte operátory IBM do seznamu operátorů, které můžete nainstalovat.

[7] Od verze 4.4 produktu IBM Cloud Pak foundational services již není vyžadováno.

Než začnete

Tato úloha předpokládá, že jste dokončili první 3 kroky “Instalace produktu IBM MQ Operator” na stránce 101.

Tuto úlohu musí provést administrátor klastru.

Informace o této úloze

Katalog IBM MQ Operator je index operátorů dostupných pro rozšíření rozhraní API klastru Red Hat OpenShift Container Platform o povolení softwarových produktů IBM .

Vyplňte buď volbu **Volba A: vzduchová mezera** , nebo volbu **Volba B: Internet**v závislosti na tom, zda je klastr v omezeném síťovém prostředí (s omezením), nebo zda má váš klastr přístup k Internetu.

Procedura

- V 9.3.4

  Volba A: vzduchová mezera Přidejte zdroj katalogu v síťovém prostředí s omezením vzduchu.

  a) Přidejte zdroj katalogu IBM MQ Operator .

  Postupujte podle pokynů v části Přidání zdrojů katalogu do klastru.

  Poznámka: Protože jste již dokončili krok instalace operátora Zrcadlové obrazy (pouze vzduchová mezera), musíte dokončit pouze krok, který používá zdroj katalogu. Příklad:

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

  b) Přidejte zdroj katalogu pro další požadované komponenty.

  Při implementaci alespoň jednoho správce front, ve kterém platí **všechny** následující příkazy, je třeba provést několik dalších nezbytných komponent:

  – Používáte verzi IBM MQ 9.3.4 nebo novější.
  – Používáte licenci IBM Cloud Pak for Integration .
  – Parametr IBM MQ Console je povolen.
  – Používáte službu IBM Cloud Pak for Integration Keycloak pro ověření a autorizaci jednotného přihlášení IBM MQ Console (SSO) (předvolba).

  Pokud jsou všechny předchozí příkazy pravdivé, pak jednotné přihlášení poskytuje Keycloak. Proto, stejně jako pro zdroj katalogu IBM MQ Operator , musíte také postupovat podle pokynů v části Přidání zdrojů katalogu do klastru pro každou z těchto dalších nezbytných komponent:

  – IBM Cloud Pak foundational services
  – Certificate Manager. Pokud jste nainstalovali verzi operátora IBM Cloud Pak foundational services před verzí 4.4, musíte zrcadlit Certificate Manager.[8]
  – IBM Cloud Pak for Integration

- **Volba B: Internet** Přidejte zdroj katalogu do prostředí, které má přístup k Internetu.

  Vytvořte `CatalogSource` pomocí rozhraní příkazového řádku OpenShift .

  Přidejte katalog použitím následujícího souboru YAML na klastr Red Hat OpenShift Container Platform .

  a) Vytvořte CatalogSource YAML.

  Uložte následující definici prostředku jako soubor s názvem `catalog_source.yaml`.

  ```
  apiVersion: operators.coreos.com/v1alpha1
  kind: CatalogSource
  metadata:
    name: ibm-operator-catalog
  ```

[8] Od verze 4.4 IBM Cloud Pak foundational services již toto zrcadlení není vyžadováno.

```
  namespace: openshift-marketplace
spec:
  displayName: IBM Operator Catalog
  image: icr.io/cpopen/ibm-operator-catalog:latest
  publisher: IBM
  sourceType: grpc
  updateStrategy:
    registryPoll:
      interval: 45m
```

b) Použijte `CatalogSource` YAML.

Proveďte to z webové konzoly Red Hat OpenShift Container Platform klepnutím na tlačítko "+" nebo pomocí příkazového řádku.

Použijte například soubor spuštěním následujícího příkazu:

```
oc apply -f catalog_source.yaml -n openshift-marketplace
```

c) Ověřit úspěšné `CatalogSource` vytvoření

Spusťte následující příkaz:

```
oc get CatalogSources ibm-operator-catalog -n openshift-marketplace
```

Tento výstup obdržíte při úspěchu:

```
NAME                    DISPLAY                TYPE   PUBLISHER    AGE
ibm-operator-catalog    IBM operator Catalog   grpc   IBM          28s
```

Výsledky

Nyní jste připraveni dokončit krok 5 instalace produktu IBM MQ Operator.

OpenShift CP4I Instalace produktu IBM MQ Operator pomocí konzoly OpenShift

Produkt IBM MQ Operator lze nainstalovat na server Red Hat OpenShift pomocí OperatorHub.

Než začnete

Tato úloha předpokládá, že jste dokončili kroky 1-4 souboru “Instalace produktu IBM MQ Operator” na stránce 101.

Postup

1. Přihlaste se ke konzole klastru Red Hat OpenShift .
2. V navigačním podokně klepněte na volbu **Operators** > **OperatorHub**.
   Zobrazí se stránka OperatorHub.
3. Do pole **Všechny položky** zadejte hodnotu "IBM MQ".
   Zobrazí se položka katalogu IBM MQ.
4. Vyberte volbu **IBM MQ**.
   Zobrazí se okno IBM MQ.
5. Klepněte na volbu **Instalovat**.
   Zobrazí se stránka Operátor instalace.
6. Zadejte následující hodnoty:
   a) Nastavte volbu **Kanál** na zvolenou verzi.

   Chcete-li určit, na který kanál operátoru se má použít, zkontrolujte “Podpora verze pro IBM MQ Operator” na stránce 11.

   b) Nastavte **Režim instalace** buď na "specifický obor názvů na klastru" (který můžete vytvořit v dalším kroku), nebo na rozsah celého klastru.

Doporučuje se vybrat rozsah pro celý klastr, protože instalace různých verzí operátoru v různých oborech názvů může vést k problémům. Obsluha je navržena jako rozšíření řídící roviny.

c) Volitelné: Pokud jste zvolili "specifický obor názvů v klastru", nastavte **Obor názvů** na hodnotu projektu (oboru názvů), do kterého chcete operátor nainstalovat.

Poznámka: Při instalaci operátoru pomocí konzoly můžete použít buď existující obor názvů, výchozí obor názvů poskytnutý operátorem, nebo vytvořit nový obor názvů. Chcete-li vytvořit nový obor názvů, můžete jej vytvořit z tohoto formuláře takto: V navigačním podokně klepněte na volbu **Domů** > **Projekty**, vyberte volbu **Vytvořit projekt**, zadejte **Název** projektu (obor názvů), který chcete vytvořit, a poté klepněte na volbu **Vytvořit**.

d) Nastavte volbu **Strategie schválení** na hodnotu Automaticky.

7. Klepněte na tlačítko **Instalovat** a počkejte na instalaci operátora.

   Po dokončení instalace vám bude poskytnuto potvrzení.

   Chcete-li ověřit instalaci, přejděte na volbu **Operátory** > **Instalované operátory**a vyberte projekt z rozevíracího seznamu **Projekty** . Stav operátora se po dokončení instalace změní na Úspěšné.

Jak pokračovat dále

Nyní jste připraveni Vytvořit tajný klíč nároku (krok 6 z “Instalace produktu IBM MQ Operator” na stránce 101).

OpenShift CP4I Instalace IBM MQ Operator pomocí rozhraní CLI Red Hat OpenShift

Produkt IBM MQ Operator lze nainstalovat do systému Red Hat OpenShift pomocí rozhraní příkazového řádku (CLI).

Než začnete

Tato úloha předpokládá, že jste dokončili kroky 1-4 souboru “Instalace produktu IBM MQ Operator” na stránce 101.

Postup

1. Přihlaste se do rozhraní příkazového řádku (CLI) Red Hat OpenShift pomocí **`oc login`**.
2. Volitelné: 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 zapotřebí pouze v případě, že chcete provést instalaci do konkrétního oboru názvů, který dosud neexistuje.

   Chcete-li vytvořit nový obor názvů v rozhraní CLI, spusťte tento příkaz:

   ```
   oc create namespace <namespace_name>
   ```

   Kde < *název_oboru názvů* > je název oboru názvů, který chcete vytvořit.
3. Zobrazte seznam operátorů dostupných pro klastr z produktu OperatorHub:

   ```
   oc get packagemanifests -n openshift-marketplace
   ```
4. Zkontrolujte soubor IBM MQ Operator , abyste ověřili jeho podporovanou **`InstallModes`** a dostupnou **`Channels`**.

   ```
   oc describe packagemanifests ibm-mq -n openshift-marketplace
   ```
5. Volitelné: Vytvořte soubor **`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 jehož odběru přihlašujete operátora, musí mít **OperatorGroup**, který odpovídá **InstallMode** operátora, ať už v režimu `Všechny obory názvů`, nebo `Jeden obor názvů`.

Pokud operátor, který chcete nainstalovat, používá režim `AllNamespaces` , pak prostor jmen `openshift-operators` již má na svém místě odpovídající **OperatorGroup** a tento krok můžete přeskočit.

Pokud operátor používá režim `SingleNamespace` a dosud nemáte na místě odpovídající **OperatorGroup** , vytvořte jej spuštěním následujícího příkazu:

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

6. Chcete-li určit, na který kanál operátoru se má použít, zkontrolujte “Podpora verze pro IBM MQ Operator” na stránce 11.
7. Nainstalujte operátora.

   Použijte následující příkaz, změňte *< ibm-mq-operator-channel>* tak, aby odpovídal kanálu pro verzi IBM MQ Operator, kterou chcete nainstalovat, a změňte *< název_oboru_názvů>* na **openshift-operators** , pokud používáte režim "AllNamespaces", nebo na obor názvů, do kterého chcete implementovat operátor IBM MQ Operator, pokud používáte režim "SingleNamespace".

   ```
   cat << EOF | oc apply -f -
   apiVersion: operators.coreos.com/v1alpha1
   kind: Subscription
   metadata:
     name: ibm-mq
     namespace: <namespace_name>
   spec:
     channel: <ibm-mq-operator-channel>
     installPlanApproval: Automatic
     name: ibm-mq
     source: ibm-operator-catalog
     sourceNamespace: openshift-marketplace
   EOF
   ```

8. Po několika minutách je nainstalován operátor. Spusťte následující příkaz, abyste ověřili, že všechny komponenty jsou ve stavu Úspěšné:

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

   Kde *< název_oboru názvů >* je **openshift-operators** , pokud používáte režim "AllNamespaces", nebo název projektu (oboru názvů), pokud používáte režim "SingleNamespace".

Jak pokračovat dále

Nyní jste připraveni Vytvořit tajný klíč nároku (krok 6 z “Instalace produktu IBM MQ Operator” na stránce 101).

OpenShift CP4I Linux Instalace produktu IBM MQ Operator 2.x v prostředí vzduchové mezery

Tento výukový program vás provede instalací produktu IBM MQ Operator 2.x do klastru Red Hat OpenShift , který nemá připojení k Internetu. Produkt IBM MQ Operator můžete nainstalovat v prostředí vzduchové mezery pomocí přenosného úložného zařízení nebo pomocí počítače typu bastion.

Než začnete

Tyto pokyny jsou určeny pro instalaci verze 2.x produktu IBM MQ Operator v prostředí vzduchové mezery. Chcete-li nainstalovat produkt IBM MQ Operator 3.0.0 a novější, viz “Instalace produktu IBM MQ Operator” na stránce 101, věnujte zvláštní pozornost krokům specifickým pro vzduchovou mezeru.

Instalace produktu IBM MQ Operator v prostředí vzduchové mezery pomocí přenosného úložného zařízení

Kroky k dokončení instalace viz Zrcadlení obrázků s přenosným úložným zařízením v dokumentaci IBM Cloud Pak for Integration. Pokud instalujete pouze produkt IBM MQ, nahraďte všechny výskyty následujících proměnných prostředí hodnotami uvedenými zde:

```
export CASE_NAME=ibm-mq
export CASE_ARCHIVE_VERSION=version_number
export CASE_INVENTORY_SETUP=ibmMQOperator
```

kde *číslo_verze* je verze případu, kterou chcete použít k instalaci vzduchové mezery. Seznam dostupných verzí případu viz https://github.com/IBM/cloud-pak/tree/master/repo/case/ibm-mq. Chcete-li určit, na který kanál operátoru se má použít, zkontrolujte “Podpora verze pro IBM MQ Operator” na stránce 11.

Instalace produktu IBM MQ Operator v prostředí vzduchové mezery pomocí počítače typu bastion

1. “Požadavky” na stránce 109
2. “Příprava registru Docker” na stránce 109
3. “Příprava opevněného (bastion) hostitele” na stránce 110
4. “Vytvoření proměnných prostředí pro instalační program a inventář obrazů” na stránce 111
5. “Stáhněte si instalační program produktu IBM MQ a inventář obrazů” na stránce 111
6. “Přihlaste se do klastru OpenShift Container Platform jako administrátor klastru.” na stránce 111
7. “Vytvoření oboru názvů Kubernetes pro IBM MQ Operator” na stránce 111
8. “Zrcadlení obrazů a konfigurace klastru” na stránce 111
9. “Nainstalujte IBM MQ Operator.” na stránce 113
10. “Implementace správce front produktu IBM MQ” na stránce 114

Požadavky

1. Musí být nainstalován klastr OpenShift Container Platform. Informace o podporovaných verzích produktu OpenShift Container Platform viz “Podpora verze pro IBM MQ Operator” na stránce 11.
2. Registr Docker musí být k dispozici. Další informace viz téma “Příprava registru Docker” na stránce 109.
3. Opevněný (bastion) server musí být nakonfigurován. Další informace viz téma “Příprava opevněného (bastion) hostitele” na stránce 110.

Příprava registru Docker

Lokální registr Docker se používá k ukládání všech obrazů v lokálním prostředí. Musíte vytvořit takový registr a zajistit, aby vyhovoval následujícím požadavkům:

- Podporuje Docker Manifest V2, Schema 2.
- Podporuje obrazy s více architekturami.
- Je přístupný jak z opevněného serveru, tak i z uzlů klastru OpenShift Container Platform.
- Má jméno uživatele a heslo uživatele, který může zapisovat do cílového registru z opevněného hostitele.

- Má jméno uživatele a heslo uživatele, který může číst z cílového registru, který se nachází na uzlech klastru Red Hat OpenShift.
- Umožňuje oddělovače cest v názvu obrazu.

Po vytvoření registru Docker musíte nakonfigurovat registr:

- Příklad jednoduchého registru je obsažen v části Vytvoření zrcadlového registru pro instalaci v omezené síti v dokumentaci k produktu Red Hat OpenShift .
- Ověřte, že každý obor názvů splňuje následující požadavky:
  - Podporuje automatické vytváření úložišť.
  - Má pověření uživatele, který může zapisovat a vytvářet úložiště. Tato pověření opevněný hostitel používá.
  - Má pověření uživatele, který může číst všechna úložiště. Klastr OpenShift Container Platform používá tato pověření.

Příprava opevněného (bastion) hostitele

Připravte opevněného hostitele (opevněný hostitelský počítač), který může přistupovat ke klastru OpenShift Container Platform, lokálnímu registru Docker a Internetu. Bastion hostitel musí být na platformě Linux for x86-64 s libovolným operačním systémem, který podporuje rozhraní IBM Cloud Pak CLI a OpenShift Container Platform CLI.

Na vašem opevněném uzlu proveďte tyto kroky:

1. Nainstalujte OpenSSL verze 1.11.1 nebo vyšší.
2. Nainstalujte Docker nebo Podman na opevněný uzel.
   - Chcete-li nainstalovat Docker, spusťte tyto příkazy:

     ```
     yum check-update
     yum install docker
     ```

   - Chcete-li nainstalovat Podman, postupujte podle pokynů k instalaci Podman
3. Nainstalujte skopieo verze 1.x.x na uzel bastion. Chcete-li nainstalovat skopeo, spusťte tyto příkazy:

   ```
   yum check-update
   yum install skopeo
   ```

4. Nainstalujte IBM Cloud Pak CLI. Nainstalujte nejnovější verzi binárního souboru na své platformě. Další informace viz cloud-pak-cli.
   a. Stáhněte binární soubor.

      ```
      wget https://github.com/IBM/cloud-pak-cli/releases/download/vversion-number/binary-file-name
      ```

      Příklad:

      ```
      wget https://github.com/IBM/cloud-pak-cli/releases/latest/download/cloudctl-linux-amd64.tar.gz
      ```

   b. Extrahujte binární soubor.

      ```
      tar -xf binary-file-name
      ```

   c. Chcete-li upravit a přesunout soubor, spusťte následující příkazy.

      ```
      chmod 755 file-name
      mv file-name /usr/local/bin/cloudctl
      ```

   d. Ověřte, že je nainstalován `cloudctl` :

      ```
      cloudctl --help
      ```

5. Nainstalujte nástroj oc OpenShift Container Platform CLI.

   Další informace viz Nástroje OpenShift Container Platform CLI

6. Vytvořte adresář, který slouží jako úložiště offline.

   Zde je uveden příklad adresáře. Tento příklad se používá v následných krocích.

   ```
   mkdir $HOME/offline
   ```

   Poznámka: Toto úložiště offline musí být trvalé, aby se zabránilo násobnému přenosu dat. Perzistence také pomáhá spustit proces zrcadlení vícekrát nebo podle plánu.

Vytvoření proměnných prostředí pro instalační program a inventář obrazů

Vytvořte následující proměnné prostředí s názvem obrazu instalačního programu a inventářem obrazů:

```
export CASE_ARCHIVE_VERSION=version_number
export CASE_ARCHIVE=ibm-mq-$CASE_ARCHIVE_VERSION.tgz
export CASE_INVENTORY=ibmMQOperator
```

Kde *version_number* je verze případu, kterou chcete použít k provedení instalace airgap. Seznam dostupných verzí případu viz https://github.com/IBM/cloud-pak/tree/master/repo/case/ibm-mq. Chcete-li určit, který kanál operátora zvolit, prohlédněte si téma Podpora verzí pro server IBM MQ Operator .

Stáhněte si instalační program produktu IBM MQ a inventář obrazů

Stáhněte si instalační program produktu `ibm-mq` a inventář obrazů na hostitele typu bastion:

```
cloudctl case save \
    --case https://github.com/IBM/cloud-pak/raw/master/repo/case/ibm-mq/$CASE_ARCHIVE_VERSION/
$CASE_ARCHIVE \
    --outputdir $HOME/offline/
```

Přihlaste se do klastru OpenShift Container Platform jako administrátor klastru.

Zde je příklad příkazu k přihlášení do klastru OpenShift Container Platform:

```
oc login cluster_host:port --username=cluster_admin_user --password=cluster_admin_password
```

Vytvoření oboru názvů Kubernetes pro IBM MQ Operator

Vytvořte proměnnou prostředí s oborem názvů pro instalaci produktu IBM MQ Operatora poté vytvořte obor názvů:

```
export NAMESPACE=ibm-mq-test
oc create namespace ${NAMESPACE}
```

Zrcadlení obrazů a konfigurace klastru

Proveďte tyto kroky, chcete-li zrcadlit obrazy a nakonfigurovat klastr:

Poznámka: V žádném příkazu nepoužívejte vlnovku v uvozovkách. Nepoužívejte například `args "--registry registry --user registry_userid --pass registry_password --inputDir ~/offline"`. Tato vlnovka se nerozbalí a vaše příkazy mohou selhat.

1. Uložte ověřovací pověření pro všechny zdrojové registry Docker.

   Všechny obrazy IBM Cloud Platform Common Services, IBM MQ Operator a IBM MQ Advanced Developer jsou uloženy do veřejných registrů, které nevyžadují ověření. Nicméně IBM MQ Advanced Server (neDeveloper), jiné produkty a komponenty třetích stran vyžadují jeden nebo více ověřených registrů. Následující registry vyžadují ověření:

   - `cp.icr.io`

- `registry.redhat.io`
- `registry.access.redhat.com`

Další informace o těchto registrech viz Vytvoření oborů názvů registru.

Chcete-li nakonfigurovat pověření pro všechny registry vyžadující ověření, musíte spustit následující příkaz. Spusťte příkaz samostatně pro každý takový registr:

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action configure-creds-airgap \
--namespace ${NAMESPACE} \
--args "--registry registry --user registry_userid --pass registry_password --inputDir $HOME/
offline"
```

Příkaz ukládá, a zachytává v mezipaměti, pověření registru do souboru ve vašem systému souborů v umístění $HOME/`.airgap/secrets`.

2. Vytvořte proměnné prostředí s použitím informací o připojení lokálního registru Docker.

```
export LOCAL_DOCKER_REGISTRY=IP_or_FQDN_of_local_docker_registry
export LOCAL_DOCKER_USER=username
export LOCAL_DOCKER_PASSWORD=password
```

Poznámka: Registr Docker používá standardní porty, např. 80 nebo 443. Pokud váš registr Docker používá nestandardní port, uveďte port pomocí syntaxe *host*:*port*. Příklad:

```
export LOCAL_DOCKER_REGISTRY=myregistry.local:5000
```

3. Nakonfigurujte tajný údaj ověření pro lokální registr Docker.

Poznámka: Tento krok je třeba provést pouze jednou.

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action configure-creds-airgap \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
{LOCAL_DOCKER_PASSWORD}"
```

Příkaz ukládá, a zachytává v mezipaměti, pověření registru do souboru ve vašem systému souborů v umístění $HOME/`.airgap/secrets`.

4. Nakonfigurujte globální tajný údaj stažení obrazu a **ImageContentSourcePolicy**.

   a. Zkontrolujte, zda je vyžadován restart uzlu.

   - V produktu OpenShift Container Platform verze 4.4 a vyšší a v nové instalaci produktu IBM MQ Operator pomocí airgap tento krok restartuje všechny uzly klastru. Prostředky klastru mohou být nedostupné, dokud není použit nový tajný údaj stažení.
   - V produktu IBM MQ Operator 1.8je CASE aktualizován tak, aby zahrnoval další zdroj zrcadlení pro obrazy. Proto se při upgradu z předchozích verzí produktu IBM MQ Operator na verzi 1.8 nebo vyšší spustí restart uzlu.
   - Chcete-li zkontrolovat, zda tento krok vyžaduje restart uzlu, přidejte volbu `--dry-run` do kódu tohoto kroku. Tím se vygeneruje nejnovější soubor **ImageContentSourcePolicy** a zobrazí se v okně konzoly (**stdout**). Pokud se **ImageContentSourcePolicy** liší od konfigurovaného klastru **ImageContentSourcePolicy**, dojde k restartování.

     ```
     cloudctl case launch \
     --case $HOME/offline/${CASE_ARCHIVE} \
     --inventory ${CASE_INVENTORY} \
     --action configure-cluster-airgap \
     --namespace ${NAMESPACE} \
     --args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
     {LOCAL_DOCKER_PASSWORD} --inputDir $HOME/offline --dryRun"
     ```

b. Chcete-li nakonfigurovat tajný klíč stažení globálního obrazu a **ImageContentSourcePolicy**, spusťte kód pro tento krok bez volby `--dry-run` :

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action configure-cluster-airgap \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
{LOCAL_DOCKER_PASSWORD} --inputDir $HOME/offline"
```

5. Ověřte, že je vytvořen prostředek **ImageContentSourcePolicy**.

```
oc get imageContentSourcePolicy
```

6. Volitelné: Používáte-li nezabezpečený registr, musíte přidat lokální registr do seznamu **insecureRegistries** klastru.

```
oc patch image.config.openshift.io/cluster --type=merge -p '{"spec":{"registrySources":
{"insecureRegistries":["'${LOCAL_DOCKER_REGISTRY}'"]}}}'
```

7. Ověřte stav uzlu klastru.

```
oc get nodes
```

Po uplatnění **imageContentsourcePolicy** a tajného údaje stažení globálního obrazu, můžete vidět stav uzlu jako **Ready**, **Scheduling** nebo **Disabled**. Počkejte, dokud všechny uzly nebudou zobrazovat stav **Ready**.

8. Zrcadlete obrazy do lokálního registru.

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action mirror-images \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
{LOCAL_DOCKER_PASSWORD} --inputDir $HOME/offline"
```

Nainstalujte IBM MQ Operator.

1. Přihlaste se na webovou konzolu klastru Red Hat OpenShift.
2. Vytvořte zdroj katalogu. Použijte stejný terminál, který provedl předchozí kroky.

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action install-catalog \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --recursive"
```

3. Ověřte, že je pro operátor instalačního programu běžných služeb vytvořen **CatalogSource**.

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

4. Nainstalujte IBM MQ Operator pomocí OLM.
   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. Chcete-li určit, na který kanál operátoru se má použít, zkontrolujte “Podpora verze pro IBM MQ Operator” na stránce 11.

f. Nastavte **Režim instalace** buď na specifický obor názvů, který jste vytvořili, nebo na rozsah celého klastru.

g. Klepněte na volbu **Odebírat**.

Produkt **IBM MQ** je přidán na stránku **Instalované operátory**.

h. Zkontrolujte stav operátoru na stránce **Instalované operátory**. Stav se změní na **Succeeded** po dokončení instalace.

Implementace správce front produktu IBM MQ

Vytvoření nového správce front pod instalovaným operátorem viz “Implementace správce front do klastru Red Hat OpenShift Container Platform” na stránce 114.

Související úlohy

“[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery” na stránce 125
V klastru Red Hat OpenShift , který nemá připojitelnost k Internetu, existují přípravné kroky, které je třeba provést před upgradem operátora nebo správce front produktu IBM MQ 2.x .

OpenShift CP4I Implementace správce front do klastru Red Hat OpenShift Container Platform

Tento příklad implementuje správce front "rychlého spuštění", který používá dočasné (dočasné) úložiště a vypíná zabezpečení produktu IBM MQ . Zprávy nejsou trvale uchovávány při restartování správce front. Konfiguraci můžete upravit tak, aby bylo možné změnit mnoho nastavení správce front.

Informace o této úloze

Tato úloha nabízí 3 volby pro implementaci správce front do adresáře OpenShift:

1. Implementujte správce front pomocí konzoly OpenShift console.
2. Implementujte správce front pomocí rozhraní OpenShift CLI.
3. Implementujte správce front pomocí konzoly IBM Cloud Pak for Integration Platform UI.

Procedura

- **Volba 1: Implementovat správce front s konzolou OpenShift .**

a) Implementujte správce front.

a. Přihlaste se ke konzole OpenShift pomocí pověření administrátora klastru Red Hat OpenShift Container Platform .

b. Změňte **Projekt** na obor názvů, kam jste nainstalovali produkt IBM MQ Operator. Z rozevíracího seznamu **Projekt** vyberte obor názvů.

c. V navigačním podokně klepněte na volbu **Operátory** > **Instalované operátory**.

d. V seznamu na panelu Instalované operátory vyhledejte a klepněte na volbu **IBM MQ**.

e. Klepněte na kartu **Správce front**.

f. Klepněte na tlačítko **Vytvořit správce front**. Zobrazí se panel vytvoření instance a nabízí dvě metody konfigurace prostředku: **Pohled Formulář** a **Pohled YAML**. Při výchozím nastavení je vybrána volba **Zobrazení formuláře** .

b) Konfigurujte správce front.

Krok 2 Volba 1: Konfigurovat v **pohledu Formulář**.

Pohled Formulář otevře formulář, který můžete použít k zobrazení nebo úpravě konfigurace prostředku.

a. Vedle položky **Licence**klepněte na šipku a rozbalte sekci přijetí licence.

b. Pokud přijmete licenční smlouvu, nastavte volbu **Přijmout licenci** na hodnotu **true** .

c. Klepnutím na šipku otevřete rozevírací seznam a vyberte licenci. 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 179. Chcete-li implementovat správce front, musíte přijmout licenci.

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

Krok 2 Volba 2: Konfigurovat v **pohledu YAML**.

Pohled YAML otevře editor obsahující ukázkový soubor YAML pro `QueueManager`. Aktualizujte hodnoty v souboru podle níže uvedených kroků.

a. Změňte `metadata.namespace` na název vašeho projektu (oboru názvů).

b. Změňte hodnotu `spec.license.license` na řetězec licence, který odpovídá vašim požadavkům. Podrobnosti o licenci viz “Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 179 .

c. Změňte `spec.license.accept` na `true` , pokud přijmete licenční smlouvu.

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

c) Ověřte vytvoření správce front.

Chcete-li ověřit, zda jste vytvořili správce front, postupujte takto:

a. Ujistěte se, že jste v oboru názvů, ve kterém jste vytvořili soubor IBM MQ Operator .

b. Na obrazovce **Domovská stránka** klepněte na volbu **Operátory** > **Instalované operátory**a poté vyberte instalovaný produkt IBM MQ Operator , pro který jste vytvořili správce front.

c. Klepněte na kartu **Správce front**. Vytvoření je dokončeno, když stav `QueueManager` je `Running`.

- **Volba 2: Implementovat správce front s rozhraním OpenShift CLI.**

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: 9.3.5.1-r2
  license:
    accept: false
    license: L-VTPK-22YZPK
    use: NonProduction
  web:
    enabled: true
  queueManager:
    name: "QUICKSTART"
    storage:
      queueManager:
        type: ephemeral
```

Důležité: Pokud přijmete licenční smlouvu, změňte hodnotu `accept: false` na `accept: true`. Podrobnosti o licenci viz “Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 179 .

Tento příklad také zahrnuje webový server implementovaný se správcem front s povolenou webovou konzolou s jednotným přihlášením v rámci produktu IBM Cloud Pak for Integration.

V 9.3.4 Od verze IBM Cloud Pak for Integration 2023.4.1, aby jednotné přihlášení fungovalo, budete nejprve muset nainstalovat další IBM Cloud Pak for Integration komponenty.

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: 9.3.5.1-r2
  license:
    accept: false
    license: L-AMRD-XH6P3Q
  web:
    enabled: true
  queueManager:
    name: "QUICKSTART"
    storage:
      queueManager:
        type: ephemeral
```

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 179 .

b) Vytvořte objekt `QueueManager` .

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

c) Ověřte vytvoření správce front.

Ověřte, že jste vytvořili správce front, provedením následujících kroků:

a. Ověřit nasazení:

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

b. Zkontrolujte stav:

```
oc describe queuemanager quickstart
```

- **Volba 3: Implementovat správce front s IBM Cloud Pak for Integration Platform UI.**

a) V prohlížeči spusťte produkt IBM Cloud Pak for Integration Platform UI.

b) V okně IBM Cloud Pak for Integration Platform UIklepněte na volbu **Vytvořit instanci**.

c) Vyberte volbu **Systém zpráv**a poté klepněte na tlačítko **Další**.

Zobrazí se panel vytvoření instance a nabízí dvě metody konfigurace prostředku: **Pohled Formulář** a **Pohled YAML**. Při výchozím nastavení je vybrána volba **Zobrazení formuláře** .

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**.

Podrobnosti o licenci viz “Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 179 . Chcete-li implementovat správce front, musíte přijmout licenci.

f) V sekci **Správce front** zkontrolujte nebo aktualizujte **Název** základního správce front. Ve starších verzích produktu IBM Cloud Pak for Integration Platform UI použijte sekci **Konfigurace správce front**.

Ve výchozím nastavení je název správce front používaný klientskými aplikacemi IBM MQ stejný jako název serveru `QueueManager`, avšak s odebranými neplatnými znaky (například spojovníky).

g) Klepněte na volbu **Vytvořit**.

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

h) Ověřte vytvoření správce front.

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

Související úlohy

“Konfigurace trasy pro připojení ke správci front mimo klastr Red Hat OpenShift” na stránce 152
Chcete-li připojit aplikaci ke správci front IBM MQ mimo klastr Red Hat OpenShift , potřebujete trasu Red Hat OpenShift . Musíte povolit TLS ve svém správci front IBM MQ a klientské aplikaci, protože SNI je k dispozici pouze v protokolu TLS, když se používá protokol TLS 1.2 nebo vyšší. Red Hat OpenShift Container Platform Router používá SNI ke směrování požadavků na správce front IBM MQ.

“Připojení k serveru IBM MQ Console implementovanému v Red Hat OpenShift” na stránce 168
Jak se připojit k serveru IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform .

“Příklady konfigurace správce front” na stránce 132
Správce front lze konfigurovat úpravou obsahu vlastního prostředku správce front.

OpenShift CP4I Odinstalace produktu IBM MQ Operator

Konzolu Red Hat OpenShift nebo rozhraní příkazového řádku můžete použít k odinstalaci produktu IBM MQ Operator z adresáře Red Hat OpenShift.

Procedura

- Volba 1: Odinstalujte produkt IBM MQ Operator pomocí konzoly OpenShift .

  Poznámka: Pokud je agent IBM MQ Operator nainstalován ve všech projektech/prostorech jmen v klastru, zopakujte kroky 2-6 následujícího postupu pro každý projekt, ve kterém chcete odstranit správce front.

  a) Přihlaste se k webové konzole Red Hat OpenShift Container Platform pomocí pověření administrátora klastru Red Hat OpenShift Container Platform .

  b) Změňte **Projekt** na obor názvů, ze kterého chcete odinstalovat produkt IBM MQ Operator. Vyberte obor názvů z rozevíracího seznamu **Projekt** .

  c) V navigačním podokně klepněte na volbu **Operátory** > **Instalované operátory**.

  d) Klepněte na operátor **IBM MQ**.

  e) Chcete-li zobrazit správce front spravované tímto produktem IBM MQ Operator, klepněte na kartu **Správci front** .

  f) Odstraňte jednoho nebo více správců front.

  Mějte na zřeteli, že i když jsou tito správci front nadále spuštěni, nemusí bez IBM MQ Operator fungovat podle očekávání.

  g) Volitelné: V případě potřeby opakujte kroky 2-6 pro každý projekt, v němž chcete odstranit správce front.

  h) Vraťte se na volbu **Operátory** > **Instalované operátory**.

  i) Vedle operátoru **IBM MQ** klepněte na tři tečky a vyberte volbu **Odinstalovat operátor**.

- Volba 2: Odinstalujte produkt IBM MQ Operator pomocí rozhraní příkazového řádku OpenShift

  a) Přihlaste se ke svému klastru Red Hat OpenShift pomocí `oc login`.

  b) Je-li IBM MQ Operator nainstalován v jednom oboru názvů, proveďte následující dílčí kroky:

  a. Ujistěte se, že jste v projektu obsahujícím soubor IBM MQ Operator , který se má odinstalovat:

  ```
  oc project <project_name>
  ```

  b. Zobrazte správce front nainstalovaného v projektu:

  ```
  oc get qmgr
  ```

c. Odstraňte jednoho nebo více správců front:

```
oc delete qmgr <qmgr_name>
```

Mějte na zřeteli, že i když jsou tito správci front nadále spuštěni, nemusí bez IBM MQ Operator fungovat podle očekávání.

d. Zobrazte instance **ClusterServiceVersion**:

```
oc get csv
```

e. Odstraňte IBM MQ **ClusterServiceVersion**:

```
oc delete csv <ibm_mq_csv_name>
```

f. Zobrazte odběry:

```
oc get subscription
```

g. Odstraňte všechny odběry:

```
oc delete subscription <ibm_mq_subscription_name>
```

h. Pokud nikdo další nepoužívá běžné služby, může být vhodné odinstalovat operátor běžných služeb a odstranit skupinu operátorů:

i) Odinstalujte operátor obecných služeb podle pokynů v části Odinstalace základních služeb v dokumentaci k produktu IBM Cloud Pak foundational services .

ii) Zobrazte skupinu operátorů:

```
oc get operatorgroup
```

iii) Odstraňte skupinu operátorů:

```
oc delete OperatorGroup <operator_group_name>
```

c) Je-li IBM MQ Operator nainstalován a k dispozici pro všechny obory názvů v klastu, proveďte následující dílčí kroky:

a. Zobrazit všechny instalované správce front:

```
oc get qmgr -A
```

b. Odstraňte jednoho nebo více správců front:

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

Mějte na zřeteli, že i když jsou tito správci front nadále spuštěni, nemusí bez IBM MQ Operator fungovat podle očekávání.

c. Zobrazte instance **ClusterServiceVersion**:

```
oc get csv -A
```

d. Odstraňte IBM MQ **ClusterServiceVersion** z klastru:

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

e. Zobrazte odběry:

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

f. Odstraňte odběry:

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

g. Volitelné: Pokud nic jiného nepoužívá obecné služby, možná budete chtít odinstalovat operátor obecných služeb. Chcete-li tak učinit, postupujte podle pokynů v části Odinstalace základních služeb v dokumentaci k produktu IBM Cloud Pak foundational services .

OpenShift Operator2.0.0 CP4I Upgrade produktu IBM MQ Operator a správců front

Existují různé procesy upgradu pro verze produktu Continuous Delivery (CD) a Long Term Support (LTS) produktu IBM MQ Operator. Dokončete krok upgradu pro váš typ implementace.

Informace o této úloze

Chcete-li provést upgrade produktu IBM MQ Operator a správců front, proveďte jeden z následujících kroků:

Procedura

- Volba 1: **Proveďte upgrade implementací na nejnovější verzi v aktuálním kanálu operátora.**

  Chcete-li upgradovat implementace produktu IBM MQ Operator na nejnovější verzi na aktuálním kanálu operátora, viz “Upgrade na nejnovější verzi zabezpečení kanálu IBM MQ Operator” na stránce 119.
- Volba 2: **Upgradovat CD implementace.**

  Chcete-li provést upgrade předchozích CD implementací produktu IBM MQ Operator na nejnovější CD verzi IBM MQ Operator (verze 3.1.3), viz “Migrace na aktuální kanál CD konzoly IBM MQ Operator” na stránce 121.

  Poznámka:

  Verze 2.0.x byla vydána jako vydání CD i LTS , takže můžete použít proceduru v “Migrace na aktuální kanál CD konzoly IBM MQ Operator” na stránce 121 k upgradu z libovolné verze 2.0.x IBM MQ Operator na nejnovější CD verzi IBM MQ Operator.

OpenShift CP4I Upgrade na nejnovější verzi zabezpečení kanálu IBM MQ Operator

Upgrade produktu IBM MQ Operator vám umožňuje upgradovat správce front.

Než začnete

Důležité: Toto téma je určeno pro upgrade implementací produktu IBM MQ Operator na nejnovější verzi zabezpečení v kanálu nasazení. Pokud to neplatí pro vaši implementaci, podívejte se na alternativní cesty upgradu popsané v části “Upgrade produktu IBM MQ Operator a správců front” na stránce 119.

V případě nasazení agenta IBM MQ Operator v klastru Red Hat OpenShift , který nemá konektivitu k Internetu, postupujte podle pokynů v části “[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery” na stránce 125.

Postup

1. Upgradujte produkt IBM MQ Operator na novější verzi.

   Máte-li nastaveny automatické upgrady, pak po vydání nového vydání zabezpečení produkt IBM MQ Operator dokončí upgrade.

   Pokud nemáte nastaveny automatické upgrady, ručně schvalte upgrade produktu IBM MQ Operator :

   - Pokud je k dispozici upgrade, **`Upgrade Status`** může být "`Upgrade k dispozici`".
   - V tomto případě může být k dispozici ovládací prvek, který můžete použít ke schválení **InstallPlan** , který upgraduje produkt IBM MQ Operator.

2. Upgradujte správce front IBM MQ na novější verzi.

   Následující tabulka popisuje nejnovější verzi správce front IBM MQ pro každý aktivní kanál operátora. Pomocí příslušné verze postupujte podle pokynů v části “Upgrade správce front IBM MQ pomocí Red Hat OpenShift” na stránce 129.

Kanál operátoru	Nejnovější správce front produktu IBM MQ
Operator2.0.0 v2.0 (LTS)	9.3.0.17-r3
Operator3.0.0 v3.1 (CD)	9.3.5.1-r2

OpenShift Operator2.0.0 CP4I Migrace na kanál LTS konzoly IBM MQ Operator

Upgrade produktu IBM MQ Operator vám umožňuje upgradovat správce front.

Než začnete

Důležité: Toto téma je určeno pro upgrade implementací 1.3.x Long Term Support (LTS) IBM MQ Operator na LTS proud IBM MQ Operator 2.0.x **pouze**. Pokud to neplatí pro vaši implementaci, podívejte se na alternativní cesty upgradu popsané v tématu Upgrade produktu IBM MQ Operator a správců front.

V případě nasazení agenta IBM MQ Operator v klastru Red Hat OpenShift , který nemá konektivitu k Internetu, postupujte podle pokynů v části “[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery” na stránce 125.

Důležité: IBM MQ Operator 2.0.x vyžaduje:

- Red Hat OpenShift Container Platform 4.12.

  Chcete-li provést upgrade, postupujte podle pokynů v části Upgrade Red Hat OpenShift.
- IBM Cloud Pak foundational services 3.19.x

Při upgradu z produktu IBM MQ Operator 1.3.x (2020.4) jsou *obě* instance správce front s více instancemi restartovány současně. K tomu dochází, když změníte verzi produktu IBM MQ na 9.2.0.5-r3-eus. Při upgradu z verze IBM MQ Operator 1.3.x na verzi 2.0.xdochází k postupné aktualizaci správce front IBM MQ . Máte-li nainstalovaný produkt IBM Cloud Pak for Integration Platform UI , existují další restarty produktu IBM MQ při změně verze produktu IBM Cloud Pak for Integration Platform UI na 2020.4.1-8-eusa na 2022.2.1-0.

Postup

1. Před použitím odkazu v kroku 2 si musíte přečíst následující základní informace pro přechod na vyšší verzi:
   - Měli byste vynechat všechny dílčí kroky pro komponenty, které jste nenainstalovali. To zahrnuje IBM Cloud Pak for Integration Platform UI , pokud toto nemáte nainstalováno.
   - Krok 2 vás přenese do dokumentace IBM Cloud Pak for Integration . Během procesu upgradu se vrátíte k následujícímu tématu IBM MQ , kde můžete provést upgrade IBM MQ Operand: Upgrade IBM MQ správce front.
   - Všem uživatelům produktu IBM MQ se doporučuje provést alespoň následující úlohy s použitím pokynů z odkazu v kroku 2 a všech dalších úloh, které se týkají vašeho prostředí:
     – Oprava IBM MQ Operator a operand (Oprava 2020.4):
       - Aktualizujte produkt IBM MQ Operator alespoň na verzi 1.3.5 v kanálu operátora v1.3-eus .
       - Přejděte na verzi IBM MQ Operand (obraz kontejneru správce front) alespoň na verzi 9.2.0.5-r3-eus.

         Poznámka: Doporučuje se aktualizovat operátor IBM MQ alespoň na tuto verzi, ale to není povinné.

- Závislosti upgradu:
  - Přejděte na vyšší verzi IBM Cloud Pak foundational services.
  - Přejděte na vyšší verzi OpenShift Container Platform.
- Upgradujte operátory:
  - Proveďte upgrade produktu IBM MQ Operator na 2.0.23.
- Proveďte upgrade schopností:
  - Upgradujte produkt IBM MQ Operand (obraz kontejneru správce front) na nejnovější verzi 9.3.0 (9.3.0.17-r3), abyste získali nejnovější opravy zabezpečení.

2. Proveďte upgrade produktu IBM MQ Operator a správců front provedením příkazu Upgrade z produktu IBM MQ Operator 1.3-eus (IBM Cloud Pak for Integration 2020.4).

Související úlohy

"[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery" na stránce 125
V klastru Red Hat OpenShift , který nemá připojitelnost k Internetu, existují přípravné kroky, které je třeba provést před upgradem operátora nebo správce front produktu IBM MQ 2.x .

"Upgrade produktu IBM MQ Operator pomocí Red Hat OpenShift" na stránce 128
Produkt IBM MQ Operator můžete upgradovat buď pomocí webové konzoly Red Hat OpenShift , nebo rozhraní příkazového řádku.

"Upgrade správce front IBM MQ pomocí Red Hat OpenShift" na stránce 129

OpenShift CP4I CD Migrace na aktuální kanál CD konzoly IBM MQ Operator

Proveďte upgrade ze starší verze IBM MQ Operator na verzi 3.1.3. Upgrade operátora vám umožňuje upgradovat správce front.

Než začnete

Toto téma je určeno pro upgrade Continuous Delivery (CD) implementací produktu IBM MQ Operator před verzí 3.1.0 na verzi 3.1.3 **pouze**. Pokud to neplatí pro vaši implementaci, podívejte se na alternativní cesty upgradu popsané v tématu Upgrade produktu IBM MQ Operator a správců front.

Chcete-li provést upgrade na produkt IBM MQ Operator 3.1.3 , musíte spustit produkt Red Hat OpenShift Container Platform 4.12 nebo novější. Chcete-li provést upgrade platformy, prohlédněte si téma Upgrade Red Hat OpenShift.

Poznámka: Podporována jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.

Postup

1. Volitelné: **Proveďte upgrade produktu IBM MQ Operator , který je momentálně ve verzi CD starší než 2.0.0.**

   Pokud je produkt IBM MQ Operator aktuálně ve verzi 1.x CD , nejprve postupujte podle pokynů v části "Migrace produktu 1.x CD IBM MQ Operator na verzi 2.0.x" na stránce 122a poté se vraťte sem, abyste provedli upgrade na nejnovější verzi produktu CD .
2. Volitelné: **Proveďte upgrade produktu IBM MQ Operator , který je momentálně ve verzi 2.2.x nebo 2.3.x na verzi 2.4.x.**

   Pokud je váš produkt IBM MQ Operator momentálně ve verzi 2.2.x nebo 2.3.x , postupujte podle příslušných kroků v části "Migrace na kanál v2.4 konzoly IBM MQ Operator" na stránce 123a poté se vraťte sem, abyste provedli upgrade na nejnovější verzi produktu CD . Všimněte si, že se jedná o povinný předem vyžadovaný krok před upgradem na verzi 3.1.3.
3. **Proveďte upgrade komponent.**

Vyberte některou z následujících možností:

- **Volba 1**: Jste-li uživatelem produktu CP4I nebo jste implementovali alespoň jednoho ze správců front pomocí licence na produkt CP4I , postupujte podle příslušných kroků **upgradujte všechny komponenty**včetně produktu IBM MQ Operator a správců front prostřednictvím vygenerovaného plánu upgradu:
  - Chcete-li provést upgrade z verze 2023.2, viz Upgrade z 2023.2 generováním plánu upgradu.
  - Chcete-li provést upgrade z verze 2022.2, prohlédněte si téma Upgrade z 2022.2 generováním plánu upgradu.
- **Volba 2**: Pro všechny ostatní uživatele:

  a. **Zrcadlové obrazy (pouze vzduchová mezera).**

  Musíte zrcadlit obrazy IBM MQ . Proveďte kroky na následujícím odkazu s použitím pouze těchto hodnot:

  ```
  export OPERATOR_PACKAGE_NAME=ibm-mq
  export OPERATOR_VERSION=3.1.3
  ```

  Měli byste vynechat sekci 3.5 "Konfigurovat klastr", protože připojení k registru obrazů by mělo být nastaveno během předchozích instalací nebo upgradů.

  Odkaz: Obrázky zrcadlení pro klastr s omezením vzduchu.

  b. **Upgradujte IBM MQ Operator na 3.1.3.**

  Viz “Upgrade produktu IBM MQ Operator pomocí Red Hat OpenShift” na stránce 128.

  c. **Proveďte upgrade instancí.**

  Chcete-li získat nejnovější funkce a opravy zabezpečení, upgradujte produkt IBM MQ Operand (obraz kontejneru správce front) na nejnovější verzi produktu CD (9.3.5.1-r2). Viz “Upgrade správce front IBM MQ pomocí Red Hat OpenShift” na stránce 129.

4. Volitelné: **Upgrade Red Hat OpenShift Container Platform 4.12 na 4.14.**

   Od verze IBM MQ Operator 3.0.0se požaduje Red Hat OpenShift Container Platform 4.12 . Všimněte si, že můžete volitelně zvolit další upgrade na verzi Red Hat OpenShift 4.14. Chcete-li ověřit kompatibilní verze pro každý kanál IBM MQ Operator , prohlédněte si téma “Kompatibilní verze Red Hat OpenShift Container Platform” na stránce 12. Chcete-li provést upgrade, prohlédněte si téma Upgrade Red Hat OpenShift.
5. Volitelné: **Ukotvte specifický zdroj katalogu pro IBM MQ Operator.**

   Pokud instalace, kterou upgradujete, používá katalog IBM MQ Operator , měli byste ukotvit specifický zdroj katalogu pro produkt IBM MQ Operator. Viz Přesun do specifických zdrojů katalogu pro každý operátor.

Související úlohy

“[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery” na stránce 125
V klastru Red Hat OpenShift , který nemá připojitelnost k Internetu, existují přípravné kroky, které je třeba provést před upgradem operátora nebo správce front produktu IBM MQ 2.x .

Operator2.2.0 OpenShift CP4I ***Migrace produktu 1.x CD IBM MQ Operator na verzi 2.0.x***

Upgrade produktu IBM MQ Operator vám umožňuje upgradovat správce front.

Než začnete

Důležité: Toto téma je určeno pro upgrade Continuous Delivery (CD) implementací produktu IBM MQ Operator před verzí 2.0.x na verzi 2.0.x **pouze**. Pokud to neplatí pro vaši implementaci, podívejte se na alternativní cesty upgradu popsané v tématu Upgrade produktu IBM MQ Operator a správců front.

V případě nasazení agenta IBM MQ Operator v klastru Red Hat OpenShift , který nemá konektivitu k Internetu, postupujte podle pokynů v části “[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery” na stránce 125.

Chcete-li dokončit tento upgrade, musí být splněny následující požadavky pro produkt IBM MQ Operator 2.0.0 :

- Red Hat OpenShift Container Platform 4.12.

  Chcete-li provést upgrade, postupujte podle pokynů v části Upgrade Red Hat OpenShift.
- IBM Cloud Pak foundational services 3.19

Postup

1. Před použitím odkazu v kroku 2 si musíte přečíst následující základní informace pro přechod na vyšší verzi:
   - Vynechte všechny dílčí kroky pro komponenty, které jste nenainstalovali. To zahrnuje IBM Cloud Pak for Integration Platform UI , pokud toto nemáte nainstalováno.
   - Krok 2 vás přenese do dokumentace IBM Cloud Pak for Integration . Během procesu upgradu se vrátíte k následujícímu tématu IBM MQ , kde můžete provést upgrade IBM MQ Operand: Upgrade IBM MQ správce front.
   - Všem uživatelům produktu IBM MQ se doporučuje provést alespoň následující úlohy s použitím pokynů z odkazu v kroku 2 a všech dalších úloh, které se týkají vašeho prostředí:
     - Oprava IBM MQ Operator a operand (Oprava 2021.4):
       - Upgradujte produkt IBM MQ Operator alespoň na verzi 1.8.0 v kanálu operátora v1.8 .
       - Přejděte na verzi IBM MQ Operand (obraz kontejneru správce front) alespoň na verzi 9.2.5.0-r3.

         Poznámka: Doporučuje se aktualizovat IBM MQ Operand na aktuální verzi (9.3.0.17-r3), ale to není povinné.
     - Závislosti upgradu:
       - Přejděte na vyšší verzi IBM Cloud Pak foundational services.
       - Přejděte na vyšší verzi OpenShift Container Platform.
     - Upgradujte operátory:
       - Proveďte upgrade produktu IBM MQ Operator na 2.0.23.
     - Proveďte upgrade schopností:
       - Upgradujte produkt IBM MQ Operand (obraz kontejneru správce front) na nejnovější verzi 9.3.0 (9.3.0.17-r3), abyste získali nejnovější opravy zabezpečení.
2. Proveďte upgrade produktu IBM MQ Operator a správců front provedením příkazu Upgrade z produktu IBM MQ Operator 1.8 (IBM Cloud Pak for Integration 2021.4) nebo starší verze produktu CD IBM MQ Operator .

Jak pokračovat dále

Nyní jste připraveni provést upgrade produktu IBM MQ Operator a správců front na nejnovější verzi produktu CD (3.1.3). Viz “Migrace na aktuální kanál CD konzoly IBM MQ Operator” na stránce 121.

Migrace na kanál v2.4 konzoly IBM MQ Operator

Upgrade produktu IBM MQ Operator vám umožňuje upgradovat správce front.

Než začnete

Důležité: Toto téma je určeno pro upgrade Continuous Delivery (CD) implementací produktu IBM MQ Operator před verzí 2.4.0na verzi 2.4.8 **pouze**. Jedná se o přechodný krok pro upgrade na nejnovější verzi produktu CD produktu IBM MQ Operator; kanál v2.4 nepřijímá aktualizace zabezpečení. Pokud to neplatí pro vaši implementaci, podívejte se na alternativní cesty upgradu popsané v tématu Upgrade produktu IBM MQ Operator a správců front.

V případě nasazení agenta IBM MQ Operator v klastru Red Hat OpenShift , který nemá konektivitu k Internetu, postupujte podle pokynů v části “[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery” na stránce 125.

Chcete-li dokončit tento upgrade, musí být splněny následující požadavky na produkt IBM MQ Operator 2.4.8 :

- Red Hat OpenShift Container Platform 4.12.

  Chcete-li provést upgrade, postupujte podle pokynů v části Upgrade Red Hat OpenShift.

  Poznámka: Podporována jsou pouze vydání OpenShift Container Platform Extended Update Support (EUS), což jsou dílčí vydání se sudým číslem, například 4.14 a 4.16.
- IBM Cloud Pak foundational services 3.19 až 3.24 včetně.

Postup

1. Volitelné: **Upgradovat produkt IBM MQ Operator , který je momentálně ve verzi CD starší než 2.0.0**

   Pokud je váš systém IBM MQ Operator momentálně na verzi 1.x CD , nejprve postupujte podle procedury v části “Migrace produktu 1.x CD IBM MQ Operator na verzi 2.0.x” na stránce 122, pak se vraťte sem a upgradujte na nejnovější verzi 2.4 .
2. **Proveďte upgrade produktu IBM MQ Operator , který je ve verzi CD 2.x.x , na nejnovější verzi 2.4 (2.4.8).**

   Postupujte podle pokynů v části “Upgrade produktu IBM MQ Operator pomocí Red Hat OpenShift” na stránce 128.
3. Volitelné: **Proveďte upgrade ostatních komponent produktu IBM Cloud Pak for Integration.**

   Pokud jste uživatelem produktu IBM Cloud Pak for Integration , můžete mít další komponenty, které chcete upgradovat. Chcete-li provést upgrade jiných komponent, postupujte podle příslušných kroků uvedených níže na základě vaší implementace:

   - Volba 1: Přechod na vyšší verzi z operátoru IBM MQ 2.0.x/2.1.x (IBM Cloud Pak for Integration 2022.2).
   - Volba 2: Přechod na vyšší verzi z operátoru IBM MQ 2.2.x/2.3.x (IBM Cloud Pak for Integration 2022.4).
4. Volitelné: **Proveďte upgrade serveru IBM Cloud Pak foundational services.**

   Pokud jste uživatelem produktu IBM Cloud Pak for Integration , možná budete chtít upgradovat produkt IBM Cloud Pak foundational services z verze 3.19.x na verzi 3.24.x. Postup dokončení tohoto upgradu viz Upgrade IBM Cloud Pak foundational services.

Související úlohy

“[Zamítnuto]Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery” na stránce 125
V klastru Red Hat OpenShift , který nemá připojitelnost k Internetu, existují přípravné kroky, které je třeba provést před upgradem operátora nebo správce front produktu IBM MQ 2.x .

“Upgrade produktu IBM MQ Operator pomocí Red Hat OpenShift” na stránce 128
Produkt IBM MQ Operator můžete upgradovat buď pomocí webové konzoly Red Hat OpenShift , nebo rozhraní příkazového řádku.

“Upgrade správce front IBM MQ pomocí Red Hat OpenShift” na stránce 129

OpenShift CP4I Linux Deprecated Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery

V klastru Red Hat OpenShift , který nemá připojitelnost k Internetu, existují přípravné kroky, které je třeba provést před upgradem operátora nebo správce front produktu IBM MQ 2.x .

Než začnete

Poznámka: Tyto pokyny jsou určeny pro upgrade na verzi 2.x produktu IBM MQ Operator v prostředí vzduchové mezery. Chcete-li přejít na verzi IBM MQ Operator 3.0.0 a novější, věnujte zvláštní pozornost krokům specifickým pro vzduchovou mezeru, viz “Upgrade produktu IBM MQ Operator a správců front” na stránce 119.

Toto téma předpokládá, že jste již nakonfigurovali lokální registr obrazů, ve kterém jsou zrcadleny dříve vydané obrazy IBM Cloud Pak for Integration .

Informace o této úloze

Než budete moci upgradovat produkt IBM MQ Operator nebo správce front v prostředí airgap, musíte zrcadlit nejnovější obrazy IBM Cloud Pak for Integration .

Všimněte si, že první čtyři kroky v této úloze jsou stejné jako kroky, které provedete, když provedete “Instalace produktu IBM MQ Operator 2.x v prostředí vzduchové mezery” na stránce 108.

Postup

1. Vytvořte proměnné prostředí pro inventář instalačního programu a obrazu.

   Vytvořte následující proměnné prostředí s názvem obrazu instalačního programu a inventářem obrazů:

   ```
   export CASE_ARCHIVE_VERSION=version_number
   export CASE_ARCHIVE=ibm-mq-$CASE_ARCHIVE_VERSION.tgz
   export CASE_INVENTORY=ibmMQOperator
   ```

   Kde *version_number* je verze případu, kterou chcete použít k provedení instalace airgap. Seznam dostupných verzí případu viz https://github.com/IBM/cloud-pak/tree/master/repo/case/ibm-mq. Chcete-li určit, který kanál operátora zvolit, prohlédněte si téma Podpora verzí pro server IBM MQ Operator .

2. Stáhněte instalační program IBM MQ a soupis obrazů.

   Stáhněte si instalační program produktu `ibm-mq` a inventář obrazů na hostitele typu bastion:

   ```
   cloudctl case save \
       --case https://github.com/IBM/cloud-pak/raw/master/repo/case/ibm-mq/
   $CASE_ARCHIVE_VERSION/$CASE_ARCHIVE \
       --outputdir $HOME/offline/
   ```

3. Přihlaste se ke klastru OpenShift Container Platform jako administrátor klastru.

   Zde je příklad příkazu k přihlášení do klastru OpenShift Container Platform:

   ```
   oc login cluster_host:port --username=cluster_admin_user --password=cluster_admin_password
   ```

4. Zrcadlete obrazy a nakonfigurujte klastr.

   Proveďte tyto kroky, chcete-li zrcadlit obrazy a nakonfigurovat klastr:

   Poznámka: V žádném příkazu nepoužívejte vlnovku v uvozovkách. Nepoužívejte například `args "--registry registry --user registry_userid --pass registry_password --inputDir ~/offline"`. Tato vlnovka se nerozbalí a vaše příkazy mohou selhat.

   a. Uložte ověřovací pověření pro všechny zdrojové registry Docker.

Všechny obrazy IBM Cloud Platform Common Services, IBM MQ Operator a IBM MQ Advanced Developer jsou uloženy do veřejných registrů, které nevyžadují ověření. Nicméně IBM MQ Advanced Server (neDeveloper), jiné produkty a komponenty třetích stran vyžadují jeden nebo více ověřených registrů. Následující registry vyžadují ověření:

- `cp.icr.io`
- `registry.redhat.io`
- `registry.access.redhat.com`

Další informace o těchto registrech viz Vytvoření oborů názvů registru.

Chcete-li nakonfigurovat pověření pro všechny registry vyžadující ověření, musíte spustit následující příkaz. Spusťte příkaz samostatně pro každý takový registr:

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action configure-creds-airgap \
--namespace ${NAMESPACE} \
--args "--registry registry --user registry_userid --pass registry_password --inputDir
$HOME/offline"
```

Příkaz ukládá, a zachytává v mezipaměti, pověření registru do souboru ve vašem systému souborů v umístění `$HOME/.airgap/secrets`.

b. Vytvořte proměnné prostředí s použitím informací o připojení lokálního registru Docker.

```
export LOCAL_DOCKER_REGISTRY=IP_or_FQDN_of_local_docker_registry
export LOCAL_DOCKER_USER=username
export LOCAL_DOCKER_PASSWORD=password
```

Poznámka: Registr Docker používá standardní porty, např. 80 nebo 443. Pokud váš registr Docker používá nestandardní port, uveďte port pomocí syntaxe *`host:port`*. Příklad:

```
export LOCAL_DOCKER_REGISTRY=myregistry.local:5000
```

c. Nakonfigurujte tajný údaj ověření pro lokální registr Docker.

Poznámka: Tento krok je třeba provést pouze jednou.

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action configure-creds-airgap \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
{LOCAL_DOCKER_PASSWORD}"
```

Příkaz ukládá, a zachytává v mezipaměti, pověření registru do souboru ve vašem systému souborů v umístění `$HOME/.airgap/secrets`.

d. Nakonfigurujte globální tajný údaj stažení obrazu a **`ImageContentSourcePolicy`**.

i) Zkontrolujte, zda je vyžadován restart uzlu.

- V produktu OpenShift Container Platform verze 4.4 a vyšší a v nové instalaci produktu IBM MQ Operator pomocí airgap tento krok restartuje všechny uzly klastru. Prostředky klastru mohou být nedostupné, dokud není použit nový tajný údaj stažení.
- V produktu IBM MQ Operator 1.8je CASE aktualizován tak, aby zahrnoval další zdroj zrcadlení pro obrazy. Proto se při upgradu z předchozích verzí produktu IBM MQ Operator na verzi 1.8 nebo vyšší spustí restart uzlu.
- Chcete-li zkontrolovat, zda tento krok vyžaduje restart uzlu, přidejte volbu `--dry-run` do kódu tohoto kroku. Tím se vygeneruje nejnovější soubor **`ImageContentSourcePolicy`**

a zobrazí se v okně konzoly (**stdout**). Pokud se **ImageContentSourcePolicy** liší od konfigurovaného klastru **ImageContentSourcePolicy**, dojde k restartování.

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action configure-cluster-airgap \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
{LOCAL_DOCKER_PASSWORD} --inputDir $HOME/offline --dryRun"
```

ii) Chcete-li nakonfigurovat tajný klíč stažení globálního obrazu a **ImageContentSourcePolicy**, spusťte kód pro tento krok bez volby `--dry-run` :

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action configure-cluster-airgap \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
{LOCAL_DOCKER_PASSWORD} --inputDir $HOME/offline"
```

e. Ověřte, že je vytvořen prostředek **ImageContentSourcePolicy**.

```
oc get imageContentSourcePolicy
```

f. Volitelné: Používáte-li nezabezpečený registr, musíte přidat lokální registr do seznamu **insecureRegistries** klastru.

```
oc patch image.config.openshift.io/cluster --type=merge -p '{"spec":{"registrySources":
{"insecureRegistries":["'${LOCAL_DOCKER_REGISTRY}'"]}}}'
```

g. Ověřte stav uzlu klastru.

```
oc get nodes
```

Po uplatnění **imageContentsourcePolicy** a tajného údaje stažení globálního obrazu, můžete vidět stav uzlu jako **Ready**, **Scheduling** nebo **Disabled**. Počkejte, dokud všechny uzly nebudou zobrazovat stav **Ready**.

h. Zrcadlete obrazy do lokálního registru.

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action mirror-images \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --user ${LOCAL_DOCKER_USER} --pass $
{LOCAL_DOCKER_PASSWORD} --inputDir $HOME/offline"
```

5. Proveďte upgrade zdroje katalogu.

Použijte stejný terminál, který provedl předchozí kroky.

```
cloudctl case launch \
--case $HOME/offline/${CASE_ARCHIVE} \
--inventory ${CASE_INVENTORY} \
--action install-catalog \
--namespace ${NAMESPACE} \
--args "--registry ${LOCAL_DOCKER_REGISTRY} --recursive"
```

Jak pokračovat dále

Chcete-li dokončit upgrade produktu IBM Cloud Pak for Integration , možná se budete muset vrátit do dokumentace k produktu IBM Cloud Pak for Integration .

V opačném případě jste nyní připraveni provést upgrade produktu IBM MQ Operator a správce front provedením jedné z následujících úloh:

- “Upgrade produktu IBM MQ Operator pomocí Red Hat OpenShift” na stránce 128

- “Upgrade správce front IBM MQ pomocí Red Hat OpenShift” na stránce 129

OpenShift CP4I Upgrade produktu IBM MQ Operator pomocí Red Hat OpenShift

Produkt IBM MQ Operator můžete upgradovat buď pomocí webové konzoly Red Hat OpenShift , nebo rozhraní příkazového řádku.

Procedura

Chcete-li provést upgrade produktu IBM MQ Operator pomocí produktu Red Hat OpenShift, proveďte jednu z následujících úloh:

- “Upgrade produktu IBM MQ Operator pomocí webové konzoly Red Hat OpenShift” na stránce 128
- “Upgrade produktu IBM MQ Operator pomocí rozhraní CLI Red Hat OpenShift” na stránce 129

OpenShift CP4I *Upgrade produktu IBM MQ Operator pomocí webové konzoly Red Hat OpenShift*

IBM MQ Operator může být upgradován pomocí Operator Hub.

Než začnete

Poznámka: Nejnovější CD verze souboru IBM MQ Operator je 3.1.3. Nejnovější LTS verze souboru IBM MQ Operator je 2.0.23. Nejnovější poznámky k verzi produktu IBM MQ Operator viz “Historie vydání pro IBM MQ Operator” na stránce 34.

Přihlaste se na webovou konzolu klastru Red Hat OpenShift.

Postup

1. Chcete-li určit, na který kanál operátoru se má upgradovat, zkontrolujte “Podpora verze pro IBM MQ Operator” na stránce 11.
2. Použít nejnovější zdroj katalogu.

   Pokud používáte specifický zdroj katalogu IBM MQ (všechny instalace vzduchové mezery), a nikoli produkt `ibm-operator-catalog`, musíte použít zdroj katalogu pro svou verzi produktu IBM MQ .

   Postupujte podle pokynů v části Přidání zdrojů katalogu do klastru.

   Poznámka: Pokud jste již dokončili krok instalace operátora pro vzduchovou mezeru Zrcadlové obrazy (pouze vzduchová mezera), musíte dokončit pouze krok, který používá zdroj katalogu. Příklad:

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

3. Upgragujte IBM MQ Operator. Nové hlavní/vedlejší verze IBM MQ Operator se dodávají prostřednictvím nových kanálů odběru. Chcete-li upgradovat operátor na novou hlavní/vedlejší verzi, budete muset aktualizovat vybraný kanál ve svém odběru IBM MQ Operator.
   a) V navigačním podokně klepněte na volbu **Operátory** > **Instalované operátory**.

      Zobrazí se všechny nainstalované operátory v uvedeném projektu.

   b) Vyberte volbu **IBM MQ Operator**.

   c) Přejděte na kartu **Odběr**.

   d) Klepněte na volbu **Kanál**.

      Zobrazí se okno **Změnit kanál aktualizace odběru**.

   e) Vyberte požadovaný kanál a klepněte na tlačítko **Uložit**.

      Operátor provede upgrade na nejnovější verzi dostupnou pro nový kanál. Viz “Podpora verze pro IBM MQ Operator” na stránce 11.

Upgrade produktu IBM MQ Operator pomocí rozhraní CLI Red Hat OpenShift

Produkt IBM MQ Operator lze upgradovat z příkazového řádku.

Než začnete

Poznámka: Nejnovější CD verze souboru IBM MQ Operator je 3.1.3. Nejnovější LTS verze souboru IBM MQ Operator je 2.0.23. Nejnovější poznámky k verzi produktu IBM MQ Operator viz “Historie vydání pro IBM MQ Operator” na stránce 34.

Přihlaste se do klastru pomocí **`oc login`**.

Než budete moci upgradovat produkt IBM MQ Operator v prostředí vzduchové mezery, musíte zrcadlit nejnovější obrazy IBM Cloud Pak for Integration . Pro upgrade na verzi IBM MQ Operator 3.0 nebo vyšší produkt Migrace na aktuální kanál CD produktu IBM MQ Operator zahrnuje kroky specifické pro vzduchovou mezeru. Chcete-li provést upgrade na starší verze operátora produktu IBM MQ , prohlédněte si téma Deprecated Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery.

Postup

1. Chcete-li určit, na který kanál operátoru se má upgradovat, zkontrolujte “Podpora verze pro IBM MQ Operator” na stránce 11.
2. Použít nejnovější zdroj katalogu.

   Pokud používáte specifický zdroj katalogu IBM MQ (všechny instalace vzduchové mezery), a nikoli produkt `ibm-operator-catalog`, musíte použít zdroj katalogu pro svou verzi produktu IBM MQ .

   Postupujte podle pokynů v části Přidání zdrojů katalogu do klastru.

   Poznámka: Pokud jste již dokončili krok instalace operátora pro vzduchovou mezeru Zrcadlové obrazy (pouze vzduchová mezera), musíte dokončit pouze krok, který používá zdroj katalogu. Příklad:

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

3. Upgragujte IBM MQ Operator. Nové hlavní/vedlejší verze IBM MQ Operator se dodávají prostřednictvím nových kanálů odběru. Chcete-li provést upgrade vašeho operátora na novou hlavní nebo vedlejší verzi, budete muset aktualizovat vybraný kanál ve svém odběru produktu IBM MQ Operator.
   a) Ujistěte se, že je k dispozici požadovaný kanál upgradu produktu IBM MQ Operator.

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

   b) Chcete-li přejít na požadovaný aktualizační kanál (kde *vX.Y* je požadovaný aktualizační kanál uvedený v předchozím kroku), proveďte opravu `Subscription`.

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

Upgrade správce front IBM MQ pomocí Red Hat OpenShift

Než začnete

V rámci procesu upgradu správců front IBM MQ jste mohli být do tohoto tématu odesláni z dokumentace k produktu IBM Cloud Pak for Integration .

Procedura

Chcete-li provést upgrade správce front IBM MQ pomocí produktu Red Hat OpenShift, proveďte jednu z následujících úloh:

- “Upgrade správce front IBM MQpomocí webové konzoly Red Hat OpenShift” na stránce 130
- “Upgrade správce front IBM MQ pomocí rozhraní CLI Red Hat OpenShift” na stránce 131
- “Upgrade správce front IBM MQ v produktu Red Hat OpenShift pomocí uživatelského rozhraní platformy” na stránce 131

Jak pokračovat dále

Chcete-li dokončit upgrade produktu IBM Cloud Pak for Integration , možná se budete muset vrátit do dokumentace k produktu IBM Cloud Pak for Integration .

OpenShift CP4I *Upgrade správce front IBM MQpomocí webové konzoly Red Hat OpenShift*

Správce front IBM MQ implementovaný pomocí IBM MQ Operator lze upgradovat v Red Hat OpenShift pomocí Operator Hub.

Než začnete

Poznámka: Nejnovější verze produktu CD správce front IBM MQ je 9.3.5.1-r2. Nejnovější verze produktu LTS správce front IBM MQ je 9.3.0.17-r3. Nejnovější poznámky k verzi správce front IBM MQ viz “Historie vydání pro obrazy kontejneru správce front pro použití s produktem IBM MQ Operator” na stránce 58.

- Přihlaste se na webovou konzolu klastru Red Hat OpenShift.
- Ujistěte se, že IBM MQ Operator používá požadovaný kanál aktualizace. Viz téma “Upgrade produktu IBM MQ Operator pomocí Red Hat OpenShift” na stránce 128.

Než budete moci provést upgrade správce front v prostředí vzduchové mezery, musíte zrcadlit nejnovější obrazy produktu IBM Cloud Pak for Integration . Pro upgrade na verzi IBM MQ Operator 3.0 nebo vyšší produkt Migrace na aktuální kanál CD produktu IBM MQ Operator zahrnuje kroky specifické pro vzduchovou mezeru. Chcete-li provést upgrade na starší verze operátora produktu IBM MQ , prohlédněte si téma Deprecated Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery.

Postup

1. V navigačním podokně klepněte na volbu **Operátory** > **Instalované operátory**.
   Zobrazí se všechny nainstalované operátory v uvedeném projektu.
2. Vyberte volbu **IBM MQ Operator**.
   Zobrazí se okno **IBM MQ Operator**.
3. Přejděte na kartu **Správce front**.
   Zobrazí se okno **Podrobnosti správce front**.
4. Vyberte správce front, kterého chcete upgradovat.
5. Přejděte na kartu YAML.
6. V případě potřeby aktualizujte následující pole tak, aby odpovídala požadovanému upgradu verze správce front IBM MQ.
   - spec.version
   - spec.license.licence

   Informace o mapování verzí produktu IBM MQ Operator a obrazů kontejnerů správce front IBM MQ naleznete v části “Historie vydání pro obrazy kontejneru správce front pro použití s produktem IBM MQ Operator” na stránce 58 .
7. Uložte aktualizovaného správce front YAML.

OpenShift CP4I *Upgrade správce front IBM MQ pomocí rozhraní CLI Red Hat OpenShift*

Správce front IBM MQ implementovaný pomocí IBM MQ Operator lze upgradovat v Red Hat OpenShift pomocí příkazového řádku.

Než začnete

Poznámka: Nejnovější verze produktu CD správce front IBM MQ je 9.3.5.1-r2. Nejnovější verze produktu LTS správce front IBM MQ je 9.3.0.17-r3. Nejnovější poznámky k verzi správce front IBM MQ viz “Historie vydání pro obrazy kontejneru správce front pro použití s produktem IBM MQ Operator” na stránce 58.

Chcete-li provést tyto kroky, musíte být administrátorem klastru.

- Přihlaste se do rozhraní příkazového řádku (CLI) produktu Red Hat OpenShift pomocí příkazu oc `login`.
- Ujistěte se, že IBM MQ Operator používá požadovaný kanál aktualizace. Viz téma “Upgrade produktu IBM MQ Operator a správců front” na stránce 119.

Než budete moci provést upgrade správce front v prostředí vzduchové mezery, musíte zrcadlit nejnovější obrazy produktu IBM Cloud Pak for Integration . Pro upgrade na verzi IBM MQ Operator 3.0 nebo vyšší produkt Migrace na aktuální kanál CD produktu IBM MQ Operator zahrnuje kroky specifické pro vzduchovou mezeru. Chcete-li provést upgrade na starší verze operátora produktu IBM MQ , prohlédněte si téma Deprecated Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery.

Postup

Upravte prostředek **QueueManager** k aktualizaci následujících polí tak, aby odpovídala požadovanému upgradu verze správce front IBM MQ.

- spec.version
- spec.license.licence

Viz “Podpora verze pro IBM MQ Operator” na stránce 11, kde jsou informace o mapování kanálů na verze IBM MQ Operator a verze správce front IBM MQ.

Zadejte následující příkaz:

```
oc edit queuemanager my_qmgr
```

Kde *my_qmgr* je název prostředku QueueManager, který chcete upgradovat.

CP4I *Upgrade správce front IBM MQ v produktu Red Hat OpenShift pomocí uživatelského rozhraní platformy*

Správce front IBM MQ implementovaný pomocí produktu IBM MQ Operator, lze upgradovat v produktu Red Hat OpenShift pomocí IBM Cloud Pak for Integration Platform UI (previously the Platform Navigator).

Než začnete

Poznámka: Nejnovější verze produktu CD správce front IBM MQ je 9.3.5.1-r2. Nejnovější verze produktu LTS správce front IBM MQ je 9.3.0.17-r3. Nejnovější poznámky k verzi správce front IBM MQ viz “Historie vydání pro obrazy kontejneru správce front pro použití s produktem IBM MQ Operator” na stránce 58.

- Přihlaste se k produktu IBM Cloud Pak for Integration Platform UI v oboru názvů, který obsahuje správce front, kterého chcete upgradovat.
- Ujistěte se, že IBM MQ Operator používá požadovaný kanál aktualizace. Viz “Upgrade produktu IBM MQ Operator a správců front” na stránce 119.

Než budete moci provést upgrade správce front v prostředí vzduchové mezery, musíte zrcadlit nejnovější obrazy produktu IBM Cloud Pak for Integration . Pro upgrade na verzi IBM MQ Operator 3.0 nebo vyšší produkt Migrace na aktuální kanál CD produktu IBM MQ Operator zahrnuje kroky specifické pro vzduchovou mezeru. Chcete-li provést upgrade na starší verze operátora produktu IBM MQ , prohlédněte si téma Deprecated Příprava na upgrade na nejnovější verzi produktu IBM MQ 2.x Operátor nebo správce front v prostředí vzduchové mezery.

Postup

1. Na domovské stránce IBM Cloud Pak for Integration Platform UI (previously the Platform Navigator) klepněte na kartu **Běhová prostředí**.
2. Správci front s dostupnými upgrady mají modré **i** vedle položky **Verze**. Klepnutím na písmeno **i** zobrazíte **K dispozici je nová verze**.
3. Klepněte na tři tečky v pravém rohu správce front, kterého chcete upgradovat, a poté klepněte na volbu **Změnit verzi**.
4. V části **Vybrat nový kanál nebo verzi** vyberte požadovanou verzi upgradu.
5. Klepněte na volbu **Změnit verzi**.

Výsledky
Správce front je upgradován.

OpenShift Konfigurace správců front pomocí konzoly IBM MQ Operator

Příklady konfigurace; konfigurace vysoké dostupnosti; připojení mimo klastr OpenShift ; integrace s řídicím panelem CP4i ; integrace s trasováním Instana; sestavení obrazu s vlastními soubory MQSC a INI; přidání vlastních anotací a štítků.

Informace o této úloze

Procedura

- “Příklady konfigurace správce front” na stránce 132.
- “Konfigurace vysoké dostupnosti pro správce front pomocí IBM MQ Operator” na stránce 141.
- “Konfigurace trasy pro připojení ke správci front mimo klastr Red Hat OpenShift” na stránce 152.
- “Integrace s IBM Cloud Pak for Integration Operations Dashboard” na stránce 154.
- “Integrace produktu IBM MQ s trasováním IBM Instana” na stránce 155.
- “Sestavení obrazu pomocí vlastních souborů MQSC a INI s použitím rozhraní CLI Red Hat OpenShift” na stránce 162.
- “Přidání vlastních anotací a štítků do prostředků správce front” na stránce 164.
- “Zakázání běhových kontrol webhooku” na stránce 164.
- “Zakázání aktualizací výchozích hodnot pro specifikaci správce front” na stránce 165.

OpenShift CP4I Příklady konfigurace správce front

Správce front lze konfigurovat úpravou obsahu vlastního prostředku správce front.

Informace o této úloze
Následující příklady vám pomohou nakonfigurovat správce front pomocí souboru QueueManager YAML.

Procedura

- “Příklad: Dodání souborů MQSC a INI” na stránce 133

- “Příklad: Konfigurace správce front s vzájemným ověřením TLS” na stránce 136

OpenShift CP4I *Příklad: Dodání souborů MQSC a INI*

Tento příklad vytvoří objekt Kubernetes ConfigMap obsahující dva soubory MQSC a jeden soubor INI. Poté je implementován správce front, který zpracovává tyto soubory MQSC a INI.

Informace o této úloze

Soubory MQSC a INI lze dodat při implementaci správce front. Data MQSC a INI musí být definována v jednom nebo více souborech Kubernetes ConfigMaps a Secrets. Ty musí být vytvořeny v oboru názvů (projekt), do kterého budete implementovat správce front.

Poznámka: Tajný klíč Kubernetes by měl být použit, když soubor MQSC nebo INI obsahuje citlivá data.

Příklad

Následující příklad vytvoří objekt Kubernetes ConfigMap obsahující dva soubory MQSC a jeden souborINI. Poté je implementován správce front, který zpracovává tyto soubory MQSC a INI.

Příklad ConfigMap - použijte následující YAML ve vašem klastru:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: mqsc-ini-example
data:
  example1.mqsc: |
    DEFINE QLOCAL('DEV.QUEUE.1') REPLACE
    DEFINE QLOCAL('DEV.QUEUE.2') REPLACE
  example2.mqsc: |
    DEFINE QLOCAL('DEV.DEAD.LETTER.QUEUE') REPLACE
  example.ini: |
    Channels:
       MQIBindType=FASTPATH
```

Příklad QueueManager -Implementujte svého správce front s následující konfigurací pomocí příkazového řádku nebo pomocí webové konzoly Red Hat OpenShift Container Platform :

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: mqsc-ini-qm
spec:
  version: 9.3.5.1-r2
  license:
    accept: false
    license: L-AMRD-XH6P3Q
    use: Production
  web:
    enabled: true
  queueManager:
    name: "MQSCINI"
    mqsc:
    - configMap:
        name: mqsc-ini-example
        items:
        - example1.mqsc
        - example2.mqsc
    ini:
    - configMap:
        name: mqsc-ini-example
        items:
        - example.ini
    storage:
      queueManager:
        type: ephemeral
```

Důležité: Pokud přijmete licenční smlouvu produktu IBM MQ Advanced, změňte `accept: false` na `accept: true`. Podrobnosti k licenci viz Odkaz na licenci pro mq.ibm.com/v1beta1.

Další informace:

- Správce front lze nakonfigurovat tak, aby používal jednu Kubernetes ConfigMap nebo Secret (jak je uvedeno v tomto příkladu) nebo více ConfigMaps a Secrets.
- Můžete zvolit použití všech dat MQSC a INI z objektu Kubernetes ConfigMap nebo Secret (jak je uvedeno v tomto příkladu) nebo můžete nakonfigurovat správce front tak, aby používal pouze dílčí sadu dostupných souborů.
- Soubory MQSC a INI se zpracovávají v abecedním pořadí podle jejich klíče. Takže `example1.mqsc` bude vždy zpracováno před `example2.mqsc`, bez ohledu na pořadí, ve kterém se objeví v konfiguraci správce front.
- Pokud má více souborů MQSC nebo INI stejný klíč napříč více objekty Kubernetes ConfigMap nebo Secret, pak je tato sada souborů zpracována dle pořadí, v němž jsou soubory definovány v konfiguraci správce front.
- Když je spuštěna sekce správce front, nejsou vyzvednuty žádné změny Kubernetes ConfigMap , protože produkt IBM MQ Operator o změně neví. Pokud provedete změny v ConfigMap, například změny v příkazech MQSC nebo v souborech INI, musíte ručně restartovat správce front, aby se tyto změny projevily. V případě správců front s jednou instancí odstraňte sekci, aby se spustil požadovaný restart. V případě nativních implementací vysoké dostupnosti nejprve restartujte pohotovostní sekce jejich odstraněním. Když jsou znovu ve spuštěném stavu, odstraňte aktivní sekci, abyste ji restartovali. Toto pořadí restartů zajišťuje minimální prostoj pro správce front.

OpenShift CP4I *Vytvoření infrastruktury PKI podepsané sebou samým pomocí OpenSSL*

Produkt IBM MQ umožňuje používat pro ověřování vzájemné zabezpečení TLS, přičemž oba konce připojení dodávají certifikát a podrobnosti v certifikátu slouží k vytvoření identity se správcem front. Toto téma uvádí, jak vytvořit ukázkovou infrastrukturu PKI (Public Key Infrastructure) pomocí nástroje příkazového řádku OpenSSL a vytvořit dva certifikáty, které lze použít v jiných příkladech.

Než začnete

Ujistěte se, že je nainstalován nástroj příkazového řádku OpenSSL .

Nainstalujte IBM MQ client a přidejte `samp/bin` a `bin` do cesty *PATH*. Potřebujete příkaz **runmqicred**, který lze nainstalovat jako součást produktu IBM MQ client , jak je uvedeno níže:

- Windows Linux Pro systémy Windows a Linux: Nainstalujte redistribuovatelného klienta IBM MQ pro váš operační systém z https://ibm.biz/mq93redistclients
- macOS Pro Mac: Stáhněte a nastavte IBM MQ MacOS Toolkit: https://developer.ibm.com/tutorials/mq-macos-dev/

Informace o této úloze

Důležité: Zde popsané příklady nejsou vhodné pro produkční prostředí a jsou určeny pouze jako příklady, jak rychle začít. Správa certifikátů je složitý předmět pro pokročilé uživatele. Pro výrobu musíte zvážit věci, jako je rotace, odvolání, délka klíče, zotavení z havárie a mnoho dalšího.

Tyto kroky byly testovány pomocí produktu OpenSSL 3.1.4.

Postup

1. Vytvořit soukromý klíč, který se má použít pro interní certifikační autoritu

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

   Soukromý klíč pro interní certifikační autoritu je vytvořen v souboru s názvem *ca.key*. Tento soubor by měl být uchováván v bezpečí a tajný-bude používán k podepisování certifikátů pro vaši interní certifikační autoritu.
2. Vydat certifikát podepsaný svým držitelem pro vaši interní certifikační autoritu

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

Parametr `-days` určuje počet dnů, po které bude kořenový certifikát certifikační autority platný.

Certifikát je vytvořen v souboru s názvem *ca.crt*. Tento certifikát obsahuje veřejné informace o interní certifikační autoritě a je volně sdílitelný.

3. Vytvořit soukromý klíč a certifikát pro správce front
   a) Vytvořit soukromý klíč a požadavek na podepsání certifikátu pro správce front

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

   Soukromý klíč je vytvořen v souboru s názvem *example-qm.key*a požadavek na podepsání certifikátu je vytvořen v souboru s názvem *example-qm.csr*

   b) Podepište klíč správce front pomocí interní certifikační autority.

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

   `-days` uvádí počet dní, po které bude certifikát platný.

   Podepsaný certifikát je vytvořen v souboru s názvem *example-qm.crt*

   c) Vytvořte tajný klíč Kubernetes s klíčem a certifikátem správce front.

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

   Vytvoří se Kubernetes tajný klíč s názvem *example-qm-tls* . Tento tajný klíč obsahuje soukromý klíč pro správce front, veřejný certifikát a certifikát CA.

4. Vytvořit soukromý klíč a certifikát pro aplikaci
   a) Vytvořit soukromý klíč a požadavek na podepsání certifikátu pro aplikaci

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

   Soukromý klíč je vytvořen v souboru s názvem *example-app1.key*a požadavek na podepsání certifikátu je vytvořen v souboru s názvem *example-app1.csr*

   b) Podepište klíč správce front pomocí interní certifikační autority.

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

   `-days` uvádí počet dní, po které bude certifikát platný.

   Podepsaný certifikát je vytvořen v souboru s názvem *example-app1.crt*

   c) Vytvořte úložiště klíčů PKCS#12 s klíčem a certifikátem aplikace.

   Produkt IBM MQ používá databázi klíčů, nikoli jednotlivé soubory klíčů. Správce front s kontejnerem vytvoří databázi klíčů pro správce front z tajného klíče, ale pro klientské aplikace je třeba databázi klíčů vytvořit ručně.

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

   Řetězec *< PASSWORD>* nahraďte heslem dle vlastního výběru.

   Úložiště klíčů je vytvořeno v souboru s názvem *example-app1.p12*. Klíč a certifikát aplikace jsou uloženy uvnitř, s "popiskem" nebo "popisným názvem"example-app1", stejně jako certifikátem CA.

   d) Používáte-li zařízení arm64 Apple Mac, musíte nakonfigurovat další soubor kombinující certifikáty aplikace a certifikační autority.
   Příklad:

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

Související úlohy

“Příklad: Konfigurace správce front s vzájemným ověřením TLS” na stránce 136
Tento příklad implementuje správce front do produktu OpenShift Container Platform pomocí IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

“Příklad: Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operator” na stránce 144
Tento příklad implementuje správce front pomocí nativní funkce vysoké dostupnosti do produktu OpenShift Container Platform pomocí konzoly IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

“Konfigurace správce front pro více instancí pomocí konzoly IBM MQ Operator” na stránce 149
Tento příklad implementuje správce front s více instancemi pomocí konzoly OpenShift Container Platform pomocí konzoly IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

OpenShift CP4I Linux *Příklad: Konfigurace správce front s vzájemným ověřením TLS*

Tento příklad implementuje správce front do produktu OpenShift Container Platform pomocí IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

Než začnete

Chcete-li dokončit tento příklad, musíte nejprve dokončit následující nezbytné předpoklady:

- V tomto příkladu vytvořte projekt/obor názvů pro OpenShift Container Platform (OCP).
- V příkazovém řádku se přihlaste ke klastru OCP a přepněte se do výše uvedeného oboru názvů.
- Ujistěte se, že je IBM MQ Operator nainstalován a k dispozici ve výše uvedeném oboru názvů.

Informace o této úloze

Tento příklad poskytuje vlastní prostředek YAML definující správce front, který má být implementován do OpenShift Container Platform. Obsahuje také podrobné informace o dalších krocích potřebných k implementaci správce front s povoleným protokolem TLS.

Postup

1. Vytvořte dvojici certifikátů, jak je popsáno v tématu “Vytvoření infrastruktury PKI podepsané sebou samým pomocí OpenSSL” na stránce 134.
2. Vytvořit mapu konfigurace obsahující příkazy MQSC a soubor INI

   Vytvořte Kubernetes ConfigMap obsahující příkazy MQSC pro vytvoření nové fronty a kanálu SVRCONN a pro přidání záznamu ověřování kanálu, který umožní přístup ke kanálu.

   Ujistěte se, že jste v prostoru jmen, který jste vytvořili dříve (viz Než začnete), pak zadejte následující YAML ve webové konzole OCP nebo pomocí příkazového řádku.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: example-tls-configmap
data:
  example-tls.mqsc: |
    DEFINE CHANNEL('MTLS.SVRCONN') CHLTYPE(SVRCONN) SSLCAUTH(REQUIRED)
SSLCIPH('ANY_TLS13_OR_HIGHER') REPLACE
    SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=*') USERSRC(NOACCESS)
ACTION(REPLACE)
    SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=example-app1') USERSRC(MAP)
MCAUSER('app1') ACTION(REPLACE)
    SET AUTHREC PRINCIPAL('app1') OBJTYPE(QMGR) AUTHADD(CONNECT,INQ)
```

```
    DEFINE QLOCAL('EXAMPLE.QUEUE') REPLACE
    SET AUTHREC PROFILE('EXAMPLE.QUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE)
AUTHADD(BROWSE,PUT,GET,INQ)
  example-tls.ini: |
    Service:
        Name=AuthorizationService
        EntryPoints=14
        SecurityPolicy=UserExternal
```

MQSC definuje kanál s názvem *MTLS.SVRCONN* a frontu s názvem *EXAMPLE.QUEUE*. Kanál je konfigurován tak, aby umožňoval přístup pouze klientům, kteří představují certifikát s "běžným názvem" *example-app1*. Jedná se o obecný název používaný v jednom z certifikátů vytvořených v kroku “1” na stránce 136. Připojení v tomto kanálu s tímto obecným názvem jsou mapována na ID uživatele *app1*, které je autorizováno pro připojení ke správci front a pro přístup k ukázkové frontě. Soubor INI povoluje zásadu zabezpečení, což znamená, že ID uživatele *app1* nemusí existovat v externím registru uživatelů-existuje pouze jako název v této konfiguraci.

3. Implementujte správce front.

   Vytvořte nového správce front s použitím následujícího vlastního prostředku YAML. Ujistěte se, že jste v oboru názvů, který jste vytvořili před zahájením této úlohy, pak zadejte následující YAML ve webové konzole OCP nebo pomocí příkazového řádku. Zkontrolujte, zda je zadána správná licence, a přijměte licenci změnou `false` na `true`.

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: exampleqm
spec:
  license:
    accept: false
    license: L-AMRD-XH6P3Q
    use: Production
  queueManager:
    name: EXAMPLEQM
    mqsc:
    - configMap:
        name: example-tls-configmap
        items:
        - example-tls.mqsc
    ini:
    - configMap:
        name: example-tls-configmap
        items:
        - example-tls.ini
    storage:
      queueManager:
        type: ephemeral
  version: 9.3.5.1-r2
  pki:
    keys:
      - name: default
        secret:
          secretName: example-qm-tls
          items:
            - tls.key
            - tls.crt
            - ca.crt
```

   Všimněte si, že tajný *příklad-qm-tls* byl vytvořen v kroku “1” na stránce 136a ConfigMap *příklad-tls-configmap* byl vytvořen v kroku “2” na stránce 136

4. Zkontrolujte, zda je správce front spuštěn.

   Správce front se nyní implementuje. Než budete pokračovat, potvrďte, že je ve stavu `Running`. Příklad:

```
oc get qmgr exampleqm
```

5. Otestujte připojení ke správci front.

   Chcete-li potvrdit, že je správce front konfigurován pro vzájemnou komunikaci TLS, postupujte podle kroků v části “Testování vzájemného připojení TLS ke správci front z přenosného počítače” na stránce 138.

Výsledky

Blahopřejeme, úspěšně jste implementovali správce front s povoleným protokolem TLS a který používá podrobnosti uvedené v certifikátu TLS k ověření u správce front a poskytnutí identity.

OpenShift CP4I Linux *Testování vzájemného připojení TLS ke správci front z přenosného počítače*

Po vytvoření správce front pomocí konzoly IBM MQ Operatormůžete otestovat, zda správce front pracuje, a to tak, že se k němu připojíte a vložíte a obdržíte zprávu. Tato úloha vás provede tím, jak se připojit pomocí ukázkových programů IBM MQ , jejich spuštěním na počítači mimo klastr Kubernetes , jako je například váš přenosný počítač.

Než začnete

Chcete-li dokončit tento příklad, musíte nejprve dokončit následující nezbytné předpoklady:

- Nainstalujte IBM MQ client. Potřebujete příkazy **amqsputc** a **amqsgetc** , které lze nainstalovat jako součást produktu IBM MQ client , jak je uvedeno níže:
  - Windows Linux Pro systémy Windows a Linux: Nainstalujte redistribuovatelného klienta IBM MQ pro váš operační systém z https://ibm.biz/mq93redistclients
  - macOS Pro Mac: Stáhněte a nastavte IBM MQ MacOS Toolkit: https://developer.ibm.com/tutorials/mq-macos-dev/
- Ujistěte se, že máte potřebné soubory s klíči a certifikáty stažené do adresáře na vašem počítači a že znáte heslo úložiště klíčů. Například tyto soubory jsou vytvořeny v adresáři “Vytvoření infrastruktury PKI podepsané sebou samým pomocí OpenSSL” na stránce 134:
  - `example-app1.p12`
  - `example-app1-chain.crt` (pouze pokud používáte zařízení arm64 Apple Mac)
- Implementujte správce front nakonfigurovaného s protokolem TLS do klastru OCP, například podle kroků v části “Příklad: Konfigurace správce front s vzájemným ověřením TLS” na stránce 136 .

Informace o této úloze

Tento příklad používá ukázkové programy IBM MQ spuštěné na počítači mimo klastr Kubernetes , jako je například váš přenosný počítač, k připojení ke správci QueueManager konfigurovanému pomocí protokolu TLS a k vložení a získání zpráv.

Postup

1. Zkontrolujte, zda je správce front spuštěn.

   Správce front se nyní implementuje. Než budete pokračovat, potvrďte, že je ve stavu `Running`. Příklad:

   ```
   oc get qmgr exampleqm
   ```

2. Najděte název hostitele správce front.

   Pomocí následujícího příkazu vyhledejte úplný název hostitele správce front pro správce front mimo klastr OCP s použitím trasy, která je vytvořena automaticky: `exampleqm-ibm-mq-qm`:

   ```
   oc get route exampleqm-ibm-mq-qm --template="{{.spec.host}}"
   ```

3. Vytvořit tabulku CCDT (Client Channel Definition Table) produktu IBM MQ

   Vytvořte soubor s názvem `ccdt.json` s následujícím obsahem:

   ```
   {
       "channel":
       [
           {
               "name": "MTLS.SVRCONN",
   ```

```
            "clientConnection":
            {
                "connection":
                [
                    {
                        "host": "<hostname from previous step>",
                        "port": 443
                    }
                ],
                "queueManager": "EXAMPLEQM"
            },
            "transmissionSecurity":
            {
              "cipherSpecification": "ANY_TLS13",
              "certificateLabel": "example-app1"
            },
            "type": "clientConnection"
        }
   ]
}
```

Připojení používá port 443, protože to je port, na kterém směrovač Red Hat OpenShift Container Platform naslouchá. Provoz bude postoupen správci front na portu 1414.

Pokud jste použili jiný název kanálu, budete jej muset také upravit. Příklady vzájemného TLS používají kanál s názvem *MTLS.SVRCONN*

Další podrobnosti viz Konfigurace formátu JSON CCDT

4. Vytvořit soubor INI klienta pro konfiguraci podrobností připojení

   Vytvořte soubor s názvem `mqclient.ini` v aktuálním adresáři. Tento soubor budou číst soubory **amqsputc** a **amqsgetc**.

```
Channels:
  ChannelDefinitionDirectory=.
  ChannelDefinitionFile=ccdt.json
SSL:
  OutboundSNI=HOSTNAME
  SSLKeyRepository=example-app1.p12
  SSLKeyRepositoryPassword=<password you used when creating the p12 file>
```

   Ujistěte se, že aktualizujete *SSLKeyRepositoryPassword* na heslo, které jste zvolili při vytváření souboru PKCS#12 . Existují i jiné způsoby, jak nastavit heslo úložiště klíčů, včetně použití šifrovaného hesla. Další informace viz Dodání hesla úložiště klíčů pro IBM MQ MQI client na AIX, Linux, and Windows

   Všimněte si, že Red Hat OpenShift Container Platform Router používá SNI pro směrování požadavků na správce front IBM MQ. Atribut *OutboundSNI= HOSTNAME* zajišťuje, že klient IBM MQ zahrne nezbytné informace, aby směrovač mohl pracovat s výchozí přenosovou cestou konfigurovanou produktem IBM MQ Operator. Další informace viz téma “Konfigurace trasy pro připojení ke správci front mimo klastr Red Hat OpenShift” na stránce 152.

5. Pokud používáte arm64 Apple Mac, musíte nakonfigurovat další proměnnou prostředí.

```
export MQSSLTRUSTSTORE=example-app1-chain.crt
```

   Tento soubor obsahuje úplný řetěz certifikátů, včetně certifikátů aplikace a CA.

6. Vložte zprávy do fronty.

   Spusťte následující příkaz:

```
/opt/mqm/samp/bin/amqsputc EXAMPLE.QUEUE EXAMPLEQM
```

   Je-li připojení ke správci front úspěšné, bude výstupem následující odezva:

```
target queue is EXAMPLE.QUEUE
```

   Vložte několik zpráv do fronty zadáním nějakého textu a následným stisknutím klávesy **Enter**.

   Chcete-li operaci dokončit, stiskněte dvakrát klávesu **Enter**.

7. Načtěte zprávy z fronty.

Spusťte následující příkaz:

```
/opt/mqm/samp/bin/amqsgetc EXAMPLE.QUEUE EXAMPLEQM
```

Zprávy, které jste přidali v předchozím kroku, byly spotřebovány a jsou výstupem. Po několika sekundách se příkaz ukončí.

Výsledky

Blahopřejeme, úspěšně jste otestovali připojení ke správci front s povoleným protokolem TLS a ukázali jste, že můžete bezpečně vkládat zprávy do správce front a získávat je z klienta.

OpenShift CP4I *Příklad: Úprava anotací služby licence*

IBM MQ Operator automaticky přidá anotace IBM License Service do implementovaných prostředků. Tyto informace jsou monitorovány produktem IBM License Service a jsou generovány sestavy, které odpovídají požadovanému oprávnění.

Informace o této úloze

Anotace přidané serverem IBM MQ Operator jsou ty, které se očekávají ve standardních situacích, a jsou založeny na hodnotách licencí vybraných během implementace správce front.

Příklad

Je-li parametr **License** nastaven na hodnotu `L-RJON-BZFQU2 (IBM Cloud Pak for Integration 2021.2.1)` a parametr **Use** je nastaven na hodnotu `Neprodukční`, jsou použity následující anotace:

- cloudpakId: c8b82d189e7545f0892db9ef2731b90d
- cloudpakName: IBM Cloud Pak for Integration
- productChargedContainers: qmgr
- productCloudpakRatio: '4:1'
- productID: 21dfe9a0f00f444f888756d835334909
- productName: IBM MQ Advanced for Non-Production
- productMetric: VIRTUAL_PROCESSOR_CORE
- productVersion: 9.2.3.0

V rámci produktu IBM Cloud Pak for Integration zahrnují implementace IBM App Connect Enterprise omezené oprávnění pro IBM MQ. V těchto situacích je třeba tyto anotace potlačit, aby bylo zajištěno, že produkt IBM License Service zachytí správné použití. Chcete-li to provést, použijte přístup popsaný v tématu “Přidání vlastních anotací a štítků do prostředků správce front” na stránce 164.

Je-li například produkt IBM MQ implementován v rámci oprávnění IBM App Connect Enterprise, použijte přístup zobrazený v následujícím fragmentu kódu:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: mq4ace
  namespace: cp4i
spec:
  annotations:
    productMetric: FREE
```

Existují dva další běžné důvody, proč mohou anotace licencí vyžadovat úpravu:

1. Produkt IBM MQ Advanced je zahrnut do oprávnění jiného produktu IBM.
   - V této situaci použijte přístup popsaný dříve pro produkt IBM App Connect Enterprise.
2. Produkt IBM MQ je implementován na základě licence IBM Cloud Pak for Integration.

- Máte-li licenci k IBM Cloud Pak for Integration, můžete rozhodnout o implementaci správce front buď v poměru IBM MQ, nebo IBM MQ Advanced. Pokud implementujete poměr IBM MQ, musíte se ujistit, že nepoužíváte žádné rozšířené schopnosti, jako je nativní HA nebo Advanced Message Security.
- V této situaci použijte následující anotace pro provozní použití:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: mq4ace
  namespace: cp4i
spec:
  annotations:
    productID: c661609261d5471fb4ff8970a36bccea
    productCloudpakRatio: '4:1'
    productName: IBM MQ for Production
    productMetric: VIRTUAL_PROCESSOR_CORE
```

- Pro neprodukční použití použijte následující anotace:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: mq4ace
  namespace: cp4i
spec:
  annotations:
    productID: 151bec68564a4a47a14e6fa99266deff
    productCloudpakRatio: '8:1'
    productName: IBM MQ for Non-Production
    productMetric: VIRTUAL_PROCESSOR_CORE
```

OpenShift MQ Adv. Konfigurace vysoké dostupnosti pro správce front pomocí IBM MQ Operator

Informace o této úloze

Procedura

- “Nativní vysoká dostupnost” na stránce 141.
- “Příklad: Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operator” na stránce 144.
- “Konfigurace správce front pro více instancí pomocí konzoly IBM MQ Operator” na stránce 149.

OpenShift MQ Adv. *Nativní vysoká dostupnost*

Nativní vysoká dostupnost je řešení nativní (vestavěné) vysoké dostupnosti pro produkt IBM MQ, které je vhodné pro použití s úložištěm bloků cloudu.

Konfigurace nativní vysoké dostupnosti poskytuje vysoce dostupného správce front, v němž jsou obnovitelná data MQ (například zprávy) replikována do více sad úložiště, a brání tak ztrátě v důsledku selhání úložiště. Správce front se skládá z více spuštěných instancí, jednou je vedoucí, další jsou připraveni rychle převzít kontrolu v případě selhání, maximalizovat přístup ke správci front a jeho zprávám.

Konfigurace nativní vysoké dostupnosti se skládá ze tří podů Kubernetes a každá s instancí správce front. Jedna instance je aktivním správcem front, zpracovává zprávy a zapisuje do svého protokolu pro zotavení. Kdykoli je zapsán protokol pro zotavení, aktivní správce front odešle data ostatním dvěma instancím, které jsou známy jako repliky. Každá replika zapisuje do svého vlastního protokolu pro zotavení, potvrzuje data a pak aktualizuje vlastní data fronty z replikovaného protokolu pro zotavení. Pokud se pod spuštěním aktivního správce front nezdaří, jedna z instancí repliky správce front převezme aktivní roli a bude mít aktuální data, se kterými bude pracovat.

Typ protokolu se nazývá 'replikovaný protokol'. Replikovaný protokol je v podstatě lineární protokol, s povolenou automatickou správou protokolů a automatickými obrazy médií. Viz Typy protokolování.

Pro správu replikovaného protokolu používáte stejné techniky, které používáte pro správu lineárního protokolu.

Služba Kubernetes se používá ke směrování připojení klienta TCP/IP k aktuální aktivní instanci, která je identifikována jako jediný pod, který je připraven pro provoz na síti. K tomu dojde bez nutnosti, aby aplikace klienta byla informována o různých instancích.

Tři pody se používají k výraznému snížení možnosti vzniku situace známé jako "split-brain". Ve dvoupodovém systému s vysokou dostupností může k rozštěpení split-brain dojít, když se přeruší propojení mezi dvěma pody. Při absenci konektivity mohou současně oba pody spustit správce front a shromáždit odlišná data. Po obnově připojení by mohly být dvě různé verze dat ('split-brain') a bylo bynutné ručním zásahem rozhodnout, která datová sada se má zachovat a která vyřadit.

Nativní vysoká dostupnost používá třípodový systém s kvótou, aby se zabránilo situaci split-brain. Pody, které mohou komunikovat alespoň s jedním z ostatních podů, tvoří kvorum. Správce front se může stát pouze aktivní instancí v podu, který má kvorum. Správce front nemůže být aktivní v podu, který není připojen k alespoň jednomu podu, takže v daném okamžiku nemohou existovat dvě aktivní instance:

- Dojde-li k nezdaru jednoho podu, může správce front na jednom z ostatních dvou podů převzít řízení. Jestliže se nezdaří dva pody, správce front se nemůže stát aktivní instancí ve zbývajícím podu, protože pod nemá kvorum (zbývající pod nemůže určit, zda ostatní dva pody se nezdařily nebo jsou stále spuštěny a bylo ztraceno připojení).
- Pokud jeden pod ztratí připojení, nemůže být správce front aktivní instancí v tomto podu, protože pod nemá kvorum. Správce front na jednom ze zbývajících dvou podů může převzít řízení, které má kvorum. Jestliže všechny pody ztratily připojení, správce front se nemůže stát aktivní instancí na některém z podů, protože žádný z podů nemá kvorum.

Pokud se aktivní pod nezdaří a následně se obnoví, může se znovu připojit ke skupině v roli repliky.

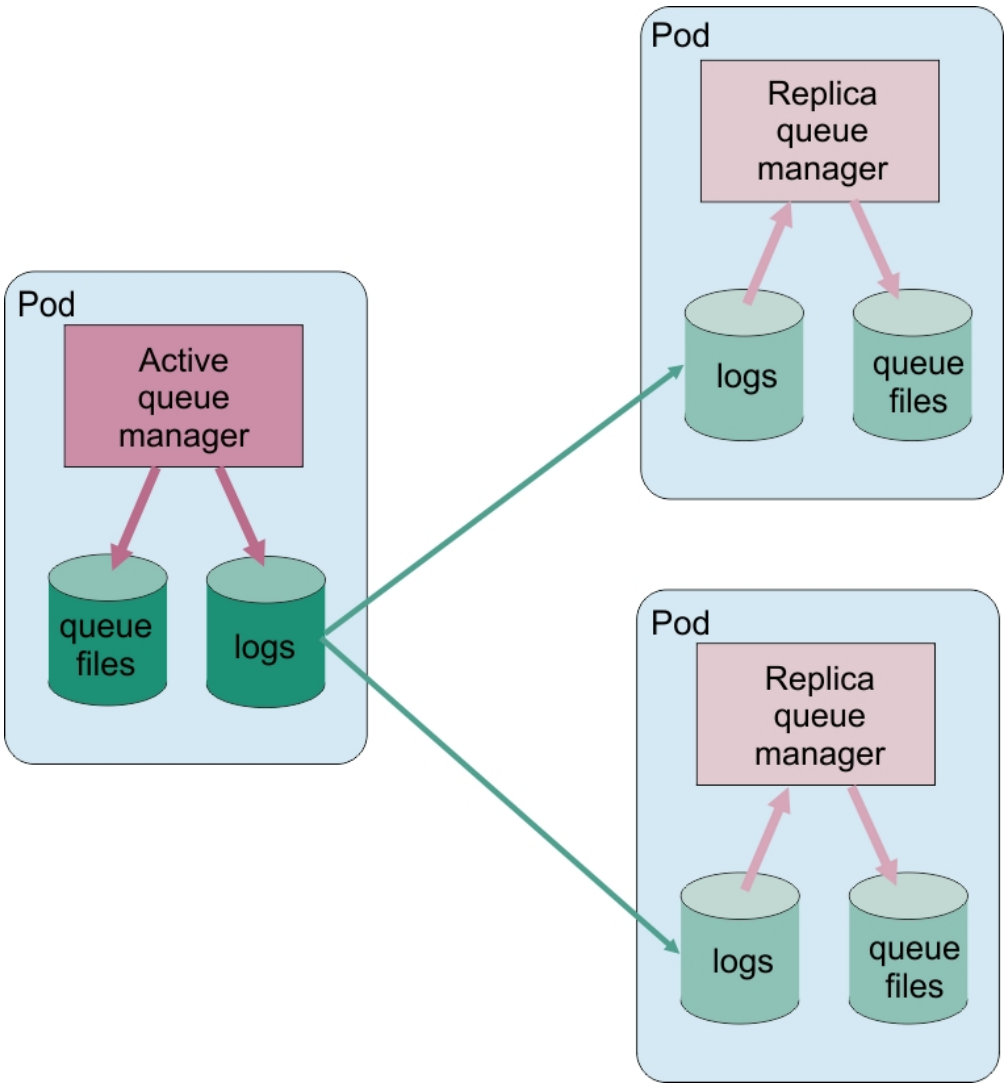
Pro výkon a spolehlivost se doporučuje trvalé úložiště RWO (ReadWriteOnce) pro použití s nativní konfigurací vysoké dostupnosti. Svazky RWO od libovolného poskytovatele úložiště jsou podporovány, pokud splňují následující podmínky:

- Získáno od poskytovatele úložiště bloků.
- Formátováno jako ext4 nebo XFS (což zajišťuje shodu se standardem POSIX).
- Podporuje dynamické zajišťování svazků a režim "volumeBinding: WaitForFirstConsumer".

Následující poskytovatelé jsou výslovně zakázáni:

- NFS
- GlusterFS
- Ostatní neblokující poskytovatelé.

Na následujícím obrázku je znázorněna typická implementace se třemi instancemi správce front implementovaného ve třech kontejnerech.



Obrázek 1. Příklad konfigurace nativní vysoké dostupnosti

OpenShift MQ Adv. *Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operator*

Nativní vysoká dostupnost je nakonfigurována pomocí rozhraní API `QueueManager` a rozšířené volby jsou k dispozici prostřednictvím souboru INI.

Nativní vysoká dostupnost je nakonfigurována pomocí `.spec.queueManager.availability` rozhraní API `QueueManager`, například:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
name: nativeha-example
spec:
  license:
    accept: false
    license: L-AMRD-XH6P3Q
    use: Production
  queueManager:
    availability:
      type: NativeHA
  version: 9.3.5.1-r2
```

Pole `.spec.queueManager.availability.type` musí být nastaveno na `NativeHA`.

Pod položkou `.spec.queueManager.availability` můžete také nakonfigurovat utajený údaj TLS a šifry, které mají být použity mezi instancemi správce front při replikaci. Tento postup se důrazně

doporučuje a podrobný průvodce je k dispozici v “Příklad: Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operator” na stránce 144.

Související úlohy

“Příklad: Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operator” na stránce 144
Tento příklad implementuje správce front pomocí nativní funkce vysoké dostupnosti do produktu OpenShift Container Platform pomocí konzoly IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

Příklad: Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operator
Tento příklad implementuje správce front pomocí nativní funkce vysoké dostupnosti do produktu OpenShift Container Platform pomocí konzoly IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

Než začnete

Chcete-li dokončit tento příklad, musíte nejprve dokončit následující nezbytné předpoklady:

- V tomto příkladu vytvořte projekt/obor názvů pro OpenShift Container Platform (OCP).
- V příkazovém řádku se přihlaste ke klastru OCP a přepněte se do výše uvedeného oboru názvů.
- Ujistěte se, že je IBM MQ Operator nainstalován a k dispozici ve výše uvedeném oboru názvů.

Informace o této úloze

Tento příklad poskytuje vlastní prostředek YAML definující správce front, který má být implementován do OpenShift Container Platform. Obsahuje také podrobné informace o dalších krocích potřebných k implementaci správce front s povoleným protokolem TLS.

Postup

1. Vytvořte dvojici certifikátů, jak je popsáno v tématu “Vytvoření infrastruktury PKI podepsané sebou samým pomocí OpenSSL” na stránce 134.
2. Vytvořit mapu konfigurace obsahující příkazy MQSC a soubor INI

   Vytvořte Kubernetes ConfigMap obsahující příkazy MQSC pro vytvoření nové fronty a kanálu SVRCONN a pro přidání záznamu ověřování kanálu, který umožní přístup ke kanálu.

   Ujistěte se, že jste v prostoru jmen, který jste vytvořili dříve (viz Než začnete), pak zadejte následující YAML ve webové konzole OCP nebo pomocí příkazového řádku.

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

   MQSC definuje kanál s názvem *MTLS.SVRCONN* a frontu s názvem *EXAMPLE.QUEUE*. Kanál je konfigurován tak, aby umožňoval přístup pouze klientům, kteří představují certifikát s "běžným

názvem" *example-app1*. Jedná se o obecný název používaný v jednom z certifikátů vytvořených v kroku “1” na stránce 144. Připojení v tomto kanálu s tímto obecným názvem jsou mapována na ID uživatele *app1*, které je autorizováno pro připojení ke správci front a pro přístup k ukázkové frontě. Soubor INI povoluje zásadu zabezpečení, což znamená, že ID uživatele *app1* nemusí existovat v externím registru uživatelů-existuje pouze jako název v této konfiguraci.

3. Implementujte správce front.

   Vytvořte nového správce front s použitím následujícího vlastního prostředku YAML. Ujistěte se, že jste v oboru názvů, který jste vytvořili před zahájením této úlohy, pak zadejte následující YAML ve webové konzole OCP nebo pomocí příkazového řádku. Zkontrolujte, zda je zadána správná licence, a přijměte licenci změnou `false` na `true`.

   ```
   apiVersion: mq.ibm.com/v1beta1
   kind: QueueManager
   metadata:
     name: exampleqm
   spec:
     license:
       accept: false
       license: L-AMRD-XH6P3Q
       use: Production
     queueManager:
       name: EXAMPLEQM
       availability:
         type: NativeHA
         tls:
           secretName: example-qm-tls
       mqsc:
       - configMap:
           name: example-nativeha-configmap
           items:
           - example-tls.mqsc
       ini:
       - configMap:
           name: example-nativeha-configmap
           items:
           - example-tls.ini
       storage:
         queueManager:
           type: persistent-claim
     version: 9.3.5.1-r2
     pki:
       keys:
         - name: default
           secret:
             secretName: example-qm-tls
             items:
               - tls.key
               - tls.crt
               - ca.crt
   ```

   Všimněte si, že tajný *příklad-qm-tls* byl vytvořen v kroku “1” na stránce 144a ConfigMap *příklad-nativeha-configmap* byl vytvořen v kroku “2” na stránce 144

   Typ dostupnosti je nastaven na *NativeHA*a je vybráno trvalé úložiště. Použije se výchozí paměťová třída nakonfigurovaná ve vašem klastru Kubernetes . Pokud nemáte nakonfigurovanou paměťovou třídu jako výchozí nastavení, nebo chcete použít jinou paměťovou třídu, přidejte `defaultClass: <storage_class_name>` pod `spec.queueManager.storage`.

   Tři pody ve správci front nativní vysoké dostupnosti replikují data po síti. Tento odkaz není standardně šifrován, ale tento příklad používá certifikát správce front pro šifrování provozu. Pro další zabezpečení můžete zadat jiný certifikát. Nativní tajný klíč TLS s vysokou dostupností musí být tajný klíč TLS Kubernetes , který má konkrétní strukturu (například soukromý klíč musí mít název *tls.key*).

4. Zkontrolujte, zda je správce front spuštěn.

   Správce front se nyní implementuje. Než budete pokračovat, potvrďte, že je ve stavu `Running`. Příklad:

   ```
   oc get qmgr exampleqm
   ```

5. Otestujte připojení ke správci front.

Chcete-li potvrdit, že je správce front nakonfigurován a dostupný, postupujte podle pokynů v části “Testování vzájemného připojení TLS ke správci front z přenosného počítače” na stránce 138.

6. Vynuťte selhání aktivního podu

   Chcete-li ověřit automatické zotavení správce front, simulujte selhání podu:

   a) Zobrazte aktivní a pohotovostní pody

      Spusťte následující příkaz:

      ```
      oc get pods --selector app.kubernetes.io/instance=exampleqm
      ```

      Všimněte si, že v poli **READY** vrací aktivní sekce hodnotu `1/1`, zatímco pody pro repliky vrací hodnotu `0/1`.

   b) Odstraňte aktivní pod

      Spusťte následující příkaz a zadejte úplný název aktivního podu:

      ```
      oc delete pod exampleqm-ibm-mq-<value>
      ```

   c) Zobrazte stav podu znovu

      Spusťte následující příkaz:

      ```
      oc get pods --selector app.kubernetes.io/instance=exampleqm
      ```

   d) Zobrazte stav správce front

      Spusťte následující příkaz a zadejte úplný název jednoho z ostatních podů:

      ```
      oc exec -t Pod -- dspmq -o nativeha -x -m EXAMPLEQM
      ```

      Měli byste vidět stav, který ukazuje, že se aktivní instance změnila, např.:

      ```
      QMNAME(EXAMPLEQM) ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
      INSTANCE(inst1) ROLE(Active) REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
      CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
      INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
      CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
      INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
      CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
      ```

   e) Znovu otestujte připojení ke správci front

      Chcete-li potvrdit zotavení správce front, postupujte podle kroků v části “Testování vzájemného připojení TLS ke správci front z přenosného počítače” na stránce 138.

Výsledky

Blahopřejeme, úspěšně jste implementovali správce front s nativní vysokou dostupností a vzájemným ověřením TLS a ověřili jste, že se při selhání aktivního podu automaticky obnoví.

OpenShift MQ Adv. *Zobrazení stavu nativních správců front HA pro kontejnery IBM MQ*

V případě kontejnerů IBM MQ můžete zobrazit stav nativních instancí vysoké dostupnosti spuštěním příkazu **dspmq** uvnitř jednoho ze spuštěných podů.

Informace o této úloze

Chcete-li zobrazit provozní stav instance správce front, můžete použít příkaz **dspmq** v jednom ze spuštěných podů. Vrácené informace závisí na tom, zda je instance aktivní nebo zda je to replika. Informace poskytnuté aktivní instancí jsou konečné, informace z replikovaných uzlů mohou být zastaralé.

Můžete provést následující akce:

- Zobrazit, zda je instance správce front v aktuálním uzlu aktivní nebo zda je to replika.
- Zobrazit provozní stav nativní vysoké dostupnosti instance v aktuálním uzlu.
- Zobrazit provozní stav všech tří instancí v konfiguraci nativní vysoké dostupnosti.

Následující stavová pole se používají k hlášení stavu konfigurace nativní vysoké dostupnosti:

ROLE
Určuje aktuální roli instance a je jednou z hodnot `Active`, `Replica` nebo `Unknown`.

INSTANCE
Název poskytnutý pro tuto instanci správce front, když byl vytvořen pomocí volby **`-lr`** příkazu **`crtmqm`**.

INSYNC
Určuje, zda je instance v případě potřeby schopna převzít funkci aktivní instance.

QUORUM
Hlásí stav kvora ve formátu *počet_synchronizovaných_instancí*/*počet_nakonfigurovaných_instancí*.

REPLADDR
Adresa replikace instance správce front.

CONNACTV
Označuje, zda je uzel připojen k aktivní instanci.

BACKLOG
Označuje, kolik kB instance překročila.

CONNINST
Označuje, zda je pojmenovaná instance připojena k této instanci.

ALTDATE
Označuje datum, kdy byly tyto informace naposledy aktualizovány (prázdné, pokud dosud nebyly aktualizovány).

ALTTIME
Označuje čas poslední aktualizace těchto informací (prázdné, pokud dosud nebyla aktualizována).

Procedura

- Vyhledejte sekce, které jsou součástí vašeho správce front.

  ```
  oc get pod --selector app.kubernetes.io/instance=nativeha-qm
  ```

- Spusťte produkt `dspmq` v jednom z podů

  ```
  oc exec -t Pod dspmq
  ```

  ```
  oc rsh Pod
  ```

  pro interaktivní shell, kde můžete spustit produkt `dspmq` přímo.

- Chcete-li určit, zda je instance správce front spuštěna jako aktivní instance nebo jako replika:

  ```
  oc exec -t Pod dspmq -o status -m QMgrName
  ```

  Aktivní instance správce front s názvem BOB bude vykazovat následující stav:

  ```
  QMNAME(BOB)                STATUS(Running)
  ```

  Instance repliky správce front s názvem BOB bude vykazovat následující stav:

  ```
  QMNAME(BOB)                STATUS(Replica)
  ```

  Neaktivní instance bude hlásit následující stav:

  ```
  QMNAME(BOB)                STATUS(Ended Immediately)
  ```

- Chcete-li určit provozní stav nativní vysoké dostupnosti instance v uvedeném modulu:

  ```
  oc exec -t Pod dspmq -o nativeha -m QMgrName
  ```

Aktivní instance správce front s názvem BOB může vykazovat následující stav:

```
QMNAME(BOB)               ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
```

Instance repliky správce front s názvem BOB může vykazovat následující stav:

```
QMNAME(BOB)               ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
```

Neaktivní instance správce front s názvem BOB může vykazovat následující stav:

```
QMNAME(BOB)               ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
```

- Chcete-li určit provozní stav nativní vysoké dostupnosti všech instancí v konfiguraci nativní vysoké dostupnosti:

```
oc exec -t Pod dspmq -o nativeha -x -m QMgrName
```

Pokud tento příkaz zadáte na uzlu, na kterém je spuštěna aktivní instance správce front BOB, můžete obdržet následující stav:

```
QMNAME(BOB)            ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

Pokud tento příkaz zadáte na uzlu, na kterém je spuštěna instance repliky správce front BOB, můžete obdržet následující stav, který znamená, že jedna z replik zaostává:

```
QMNAME(BOB)            ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(No)  BACKLOG(435)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

Pokud tento příkaz zadáte na uzlu, kde je spuštěna neaktivní instance správce front BOB, můžete obdržet následující stav:

```
QMNAME(BOB)            ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
 INSTANCE(inst1) ROLE(Unknown) REPLADDR(9.20.123.45) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst2) ROLE(Unknown) REPLADDR(9.20.123.46) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst3) ROLE(Unknown) REPLADDR(9.20.123.47) CONNACTV(No) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
```

Pokud zadáte příkaz, když se instance ještě domlouvají, která je aktivní a které jsou repliky, obdržíte následující stav:

```
QMNAME(BOB)              STATUS(Negotiating)
```

Související úlohy

“Příklad: Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operator” na stránce 144
Tento příklad implementuje správce front pomocí nativní funkce vysoké dostupnosti do produktu OpenShift Container Platform pomocí konzoly IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

Související odkazy

dspmq (display queue managers) command

OpenShift MQ Adv. *Rozšířené vyladění pro nativní vysokou dostupnost*

Rozšířené nastavení pro ladění časování a intervalů. Tato nastavení by se nemusela použít, pokud není známo, že výchozí hodnoty neodpovídají požadavkům vašeho systému.

Základní volby pro konfiguraci Nativní vysoké dostupnosti jsou zpracovávány pomocí rozhraní API `QueueManager`, které produkt IBM MQ Operator používá ke konfiguraci základních souborů INI správce front. V sekci NativeHALocalInstance stanzajsou některé další rozšířené volby, které lze konfigurovat pouze pomocí souboru INI. Další informace o konfiguraci souboru INI naleznete v části “Příklad: Dodání souborů MQSC a INI” na stránce 133 .

`HeartbeatInterval`
: Interval prezenčního signálu definuje, jak často, v milisekundách, aktivní instance správce front nativní vysoké dostupnosti odešle synchronizaci sítě. Platný rozsah hodnoty intervalu prezenčního signálu je 500 (0,5 s) do 60000 (1 min), hodnota mimo tento rozsah způsobí, že se správce front nespustí. Je-li tento atribut vynechán, použije se výchozí hodnota 5000 (5 s). Každá instance musí používat stejný interval prezenčního signálu.

`HeartbeatTimeout`
: Časový limit prezenčního signálu definuje, jak dlouho bude instance repliky správce front nativní vysoké dostupnosti čekat, než se rozhodne, že aktivní instance nereaguje. Platný rozsah hodnoty časového limitu intervalu prezenčního signálu je 500 (0,5 s) do 120000 (2 min). Hodnota časového limitu prezenčního signálu musí být větší než nebo rovna intervalu prezenčního signálu.

  Neplatná hodnota způsobí, že se správce front nespustí. Je-li tento atribut vynechán, čeká replika 2 x `HeartbeatInterval` před spuštěním procesu pro výběr nové aktivní instance. Každá instance musí používat stejný časový limit prezenčního signálu.

`RetryInterval`
: Interval opakování definuje, jak často by se měl správce front nativní vysoké dostupnosti, v milisekundách, opakovat nezdařený odkaz na replikaci. Platný rozsah intervalu opakování je 500 (0,5 s) do 120000 (2 min). Je-li tento atribut vynechán, čeká replika 2 x `HeartbeatInterval` před zopakováním nezdařeného odkazu na replikaci.

OpenShift MQ Adv. *Ukončení nativních správců front HA*

Pomocí příkazu **endmqm** můžete ukončit aktivního nebo replikovaného správce front, který je součástí nativní skupiny HA.

Procedura

- Chcete-li ukončit aktivní instanci správce front, viz téma Ukončení nativních správců front HA v sekci Konfigurace v této dokumentaci.

OpenShift CP4I MQ Adv. Kubernetes

Konfigurace správce front pro více instancí pomocí konzoly IBM MQ Operator

Tento příklad implementuje správce front s více instancemi pomocí konzoly OpenShift Container Platform pomocí konzoly IBM MQ Operator. Vzájemné zabezpečení TLS se používá pro ověření k mapování z certifikátu TLS na identitu ve správci front.

Než začnete

Chcete-li dokončit tento příklad, musíte nejprve dokončit následující nezbytné předpoklady:

- V tomto příkladu vytvořte projekt/obor názvů pro OpenShift Container Platform (OCP).
- V příkazovém řádku se přihlaste ke klastru OCP a přepněte se do výše uvedeného oboru názvů.
- Ujistěte se, že je IBM MQ Operator nainstalován a k dispozici ve výše uvedeném oboru názvů.

Informace o této úloze

Tento příklad poskytuje vlastní prostředek YAML definující správce front, který má být implementován do OpenShift Container Platform. Obsahuje také podrobné informace o dalších krocích potřebných k implementaci správce front s povoleným protokolem TLS.

Postup

1. Určit vhodnou paměťovou třídu

   K úložišti v klastru Kubernetes lze přistupovat pomocí více režimů přístupu k trvalým svazkům. Správce front s více instancemi vytváří více trvalých svazků: jeden pro každého správce front a alespoň jeden sdílený svazek. Sdílený svazek pro správce front s více instancemi musí používat paměťovou třídu `ReadWriteMany` . Výchozí paměťová třída v klastru Kubernetes je obvykle pro paměťovou třídu `ReadWriteOnce` (úložiště bloků). Pokud například používáte Red Hat OpenShift Data Foundation, paměťová třída *ocs-storagecluster-cephfs* poskytuje vhodný sdílený systém souborů. Volba souborového systému je velmi důležitá, protože ne všechny sdílené souborové systémy obsluhují zamykání souborů stejným způsobem. Viz Plánování podpory systémů souborů na platformě Multiplatforms a Testování příkazů pro systémy souborů správce front IBM MQ s více instancemi.
2. Vytvořte dvojici certifikátů, jak je popsáno v tématu “Vytvoření infrastruktury PKI podepsané sebou samým pomocí OpenSSL” na stránce 134.
3. Vytvořit mapu konfigurace obsahující příkazy MQSC a soubor INI

   Vytvořte Kubernetes ConfigMap obsahující příkazy MQSC pro vytvoření nové fronty a kanálu SVRCONN a pro přidání záznamu ověřování kanálu, který umožní přístup ke kanálu.

   Ujistěte se, že jste v prostoru jmen, který jste vytvořili dříve (viz Než začnete), pak zadejte následující YAML ve webové konzole OCP nebo pomocí příkazového řádku.

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

   MQSC definuje kanál s názvem *MTLS.SVRCONN* a frontu s názvem *EXAMPLE.QUEUE*. Kanál je konfigurován tak, aby umožňoval přístup pouze klientům, kteří představují certifikát s "běžným názvem" *example-app1*. Jedná se o obecný název používaný v jednom z certifikátů vytvořených v kroku “2” na stránce 150. Připojení v tomto kanálu s tímto obecným názvem jsou mapována na ID uživatele *app1*, které je autorizováno pro připojení ke správci front a pro přístup k ukázkové frontě. Soubor INI povoluje zásadu zabezpečení, což znamená, že ID uživatele *app1* nemusí existovat v externím registru uživatelů-existuje pouze jako název v této konfiguraci.
4. Implementujte správce front.

   Vytvořte nového správce front s použitím následujícího vlastního prostředku YAML. Ujistěte se, že jste v oboru názvů, který jste vytvořili před zahájením této úlohy, pak zadejte následující YAML ve webové konzole OCP nebo pomocí příkazového řádku. Zkontrolujte, zda je zadána správná licence, a přijměte licenci změnou `false` na `true`.

   ```
   apiVersion: mq.ibm.com/v1beta1
   kind: QueueManager
   ```

```
metadata:
  name: exampleqm
spec:
  license:
    accept: false
    license: L-AMRD-XH6P3Q
    use: Production
  queueManager:
    name: EXAMPLEQM
    availability:
      type: MultiInstance
    mqsc:
    - configMap:
        name: example-miqm-configmap
        items:
        - example-tls.mqsc
    ini:
    - configMap:
        name: example-miqm-configmap
        items:
        - example-tls.ini
    storage:
      defaultClass: <STORAGE CLASS>
  version: 9.3.5.1-r2
  pki:
    keys:
      - name: default
        secret:
          secretName: example-qm-tls
          items:
            - tls.key
            - tls.crt
            - ca.crt
```

Změňte hodnotu < STORAGE CLASS> na paměťovou třídu, kterou jste identifikovali v kroku “1” na stránce 150.

Všimněte si, že tajný *příklad-qm-tls* byl vytvořen v kroku “2” na stránce 150a ConfigMap *příklad-miqm-configmap* byl vytvořen v kroku “3” na stránce 150

Typ dostupnosti je nastaven na *MultiInstance*, což způsobí automatický výběr trvalého úložiště.

5. Zkontrolujte, zda je správce front spuštěn.

   Správce front se nyní implementuje. Než budete pokračovat, potvrďte, že je ve stavu `Running`. Příklad:

   ```
   oc get qmgr exampleqm
   ```

6. Otestujte připojení ke správci front.

   Chcete-li potvrdit, že je správce front nakonfigurován a dostupný, postupujte podle pokynů v části “Testování vzájemného připojení TLS ke správci front z přenosného počítače” na stránce 138.

7. Vynuťte selhání aktivního podu

   Chcete-li ověřit automatické zotavení správce front, simulujte selhání podu:

   a) Zobrazte aktivní a pohotovostní pody

      Spusťte následující příkaz:

      ```
      oc get pods --selector app.kubernetes.io/instance=exampleqm
      ```

      Všimněte si, že v poli **READY** aktivní pod vrací hodnotu `1/1`, zatímco rezervní pod vrací hodnotu `0/1`.

   b) Odstraňte aktivní pod

      Spusťte následující příkaz a zadejte úplný název aktivního podu:

      ```
      oc delete pod exampleqm-ibm-mq-<value>
      ```

   c) Zobrazte stav podu znovu

      Spusťte následující příkaz:

      ```
      oc get pods --selector app.kubernetes.io/instance=exampleqm
      ```

d) Zobrazte stav správce front

Spusťte následující příkaz a zadejte úplný název jiné sekce:

```
oc exec -t Pod -- dspmq -x
```

Měli byste vidět stav, který ukazuje, že se aktivní instance změnila, např.:

```
QMNAME(EXAMPLEQM)                                         STATUS(Running as standby)
    INSTANCE(exampleqm-ibm-mq-1) MODE(Active)
    INSTANCE(exampleqm-ibm-mq-0) MODE(Standby)
```

e) Znovu otestujte připojení ke správci front

Chcete-li potvrdit zotavení správce front, postupujte podle kroků v části “Testování vzájemného připojení TLS ke správci front z přenosného počítače” na stránce 138.

Výsledky

Blahopřejeme, úspěšně jste implementovali správce front s více instancemi se vzájemným ověřením TLS a ověřili jste, že se automaticky obnoví, když dojde k selhání aktivního podu.

OpenShift CP4I CD V 9.3.0 Konfigurace trasy pro připojení ke správci front mimo klastr Red Hat OpenShift

Chcete-li připojit aplikaci ke správci front IBM MQ mimo klastr Red Hat OpenShift , potřebujete trasu Red Hat OpenShift . Musíte povolit TLS ve svém správci front IBM MQ a klientské aplikaci, protože SNI je k dispozici pouze v protokolu TLS, když se používá protokol TLS 1.2 nebo vyšší. Red Hat OpenShift Container Platform Router používá SNI ke směrování požadavků na správce front IBM MQ.

Informace o této úloze

Požadovaná konfigurace Red Hat OpenShift Trasa závisí na chování SNI (Server Name Indication) (SNI) vaší klientské aplikace. IBM MQ podporuje dvě různá nastavení záhlaví SNI v závislosti na konfiguraci a typu klienta. Záhlaví SNI je nastaveno na název hostitele místa určení klienta nebo na název kanálu IBM MQ . Informace, jak IBM MQ mapuje název kanálu na název hostitele, viz Jak IBM MQ poskytuje schopnost s více certifikáty.

Zda je záhlaví SNI nastaveno na název kanálu IBM MQ nebo název hostitele je řízeno pomocí atributu **OutboundSNI** . Možné hodnoty jsou `OutboundSNI=CHANNEL` (výchozí hodnota) nebo `OutboundSNI=HOSTNAME`. Další informace viz Sekce SSL konfiguračního souboru klienta. Všimněte si, že `CHANNEL` a `HOSTNAME` jsou přesné hodnoty, které používáte; nejedná se o názvy proměnných, které nahradíte skutečným názvem kanálu nebo názvem hostitele.

Chování klienta s různými nastaveními `OutboundSNI`

Je-li parametr **OutboundSNI** nastaven na `HOSTNAME`, následující klienti nastaví název hostitele SNI, pokud je v názvu připojení uveden název hostitele:

- Klienti C
- Klienti .NET v nespravovaném režimu
- Klienti Java/JMS

Je-li parametr **OutboundSNI** nastaven na hodnotu `HOSTNAME` a v názvu připojení se používá adresa IP, následující klienti odesílají prázdné záhlaví SNI:

- Klienti C
- Klienti .NET v nespravovaném režimu
- Klienti Java/JMS (nelze provést zpětné vyhledání DNS názvu hostitele)

Je-li parametr **OutboundSNI** nastaven na `CHANNEL` nebo není nastaven, použije se místo něj název kanálu IBM MQ a je vždy odesláno, zda je použit název hostitele nebo název připojení s adresou IP.

Následující typy klientů nepodporují nastavení záhlaví SNI pro název kanálu IBM MQ, a tak se vždy pokuste nastavit záhlaví SNI na název hostitele bez ohledu na nastavení parametru **OutboundSNI**:

- Klienti AMQP
- Klienti XR
- Klienti .NET ve spravovaném režimu (před IBM MQ 9.3.0)

V systému IBM MQ 9.3.0byl klient IBM MQ spravovaný .NET aktualizován tak, aby nastavil SERVERNAME na odpovídající název hostitele, pokud je vlastnost **OutboundSNI** nastavena na hodnotu HOSTNAME, což umožňuje klientovi IBM MQ spravovanému .NET připojení ke správci front pomocí tras produktu Red Hat OpenShift .

Pokud se aplikace klienta připojuje ke správci front implementovanému v klastru Red Hat OpenShift prostřednictvím IBM MQ Internet Pass-Thru (MQIPT), může být MQIPT konfigurován tak, aby nastavil SNI na název hostitele pomocí vlastnosti SSLClientOutboundSNI v definici předepsané cesty.

OutboundSNI, více certifikátů a Red Hat OpenShift tras

Produkt IBM MQ používá záhlaví SNI k zajištění funkčnosti více certifikátů. Pokud se aplikace připojuje ke kanálu IBM MQ , který je konfigurován pro použití jiného certifikátu prostřednictvím pole CERTLABL, musí se aplikace připojit s nastavením **OutboundSNI** na hodnotu CHANNEL.

Pokud vaše konfigurace přenosové cesty Red Hat OpenShift vyžaduje HOSTNAME SNI, nemůžete použít funkci více certifikátů produktu IBM MQ a nemůžete nastavit nastavení CERTLABL na žádném objektu kanálu IBM MQ .

Pokud se aplikace s nastavením **OutboundSNI** na jinou hodnotu než CHANNEL připojí ke kanálu s nakonfigurovaným popiskem certifikátu, aplikace se odmítne s hodnotou MQRC_SSL_INITIALIZATION_ERROR a v protokolech chyb správce front se zobrazí zpráva AMQ9673 .

Další informace o tom, jak produkt IBM MQ poskytuje více funkcí certifikátu, naleznete v tématu Jak IBM MQ poskytuje více možností certifikátů .

Příklad

Aplikace klienta, které nastavují SNI na kanál MQ, vyžadují vytvoření nového Red Hat OpenShift Route pro každý kanál, ke kterému se chcete připojit. Musíte také použít jedinečné názvy kanálů napříč klastrem Red Hat OpenShift Container Platform, což umožňuje směrování do správného správce front.

Je důležité, aby názvy kanálů produktu MQ nekončíaly malými písmeny, protože IBM MQ mapuje názvy kanálů na záhlaví SNI.

Chcete-li určit požadovaný název hostitele pro každý z vašich nových Red Hat OpenShift Routes, je třeba mapovat každý název kanálu na adresu SNI. Další informace viz Jak IBM MQ poskytuje schopnost s více certifikáty.

Potom musíte pro každý kanál vytvořit nový Red Hat OpenShift Route 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 "<Queue Manager
Name>-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 "<Queue Manager Name>-ibm-mq-qm")>
-n <namespace of your MQ deployment> -o jsonpath="{.spec.host}"
```

Port pro připojení klienta by měl být nastaven na port, který používá Red Hat OpenShift Container Platform Router - běžně 443.

Související úlohy

“Připojení k serveru IBM MQ Console implementovanému v Red Hat OpenShift” na stránce 168
Jak se připojit k serveru IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform .

Deprecated CP4I Removed Integrace s IBM Cloud Pak for Integration Operations Dashboard

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

Než začnete

Upozornění:

Deprecated V 9.3.0 V 9.3.0 Od verze IBM MQ Operator 2.0.0 je řídicí panel operací zamítnutý a neobdrží žádné další aktualizace. Neměla by se vytvářet žádná nová použití řídicího panelu operací.

V 9.3.3 Removed Z produktu IBM MQ Operator 2.4.0 je odebrán řídicí panel Operace. Mějte na paměti, že panel dashboard operací lze nadále používat pro existující správce front, kteří jsou starší než 9.3.3.0-r1 , pokud se nacházejí v systému IBM MQ Operator podporujícím daný obraz kontejneru správce front. Informace o podpoře verze pro produkt IBM MQ Operatornaleznete v části “Dostupné verze produktu IBM MQ” na stránce 12.

Podpora pro řídicí panel operací končí 30. června 2024. Další informace naleznete v tématu Odstoupení od softwaru a/nebo ukončení podpory.

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 UI (previously the 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. Další informace o implementaci správce front naleznete v tématu Implementace správce front s produktem IBM Cloud Pak for Integration Platform UI .

   Pokud implementujete pomocí Red Hat OpenShift CLI nebo Red Hat OpenShift webové konzoly, pak můžete povolit trasování s následujícím úsekem kódu YAML:

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

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 prvního správce front s integrací produktu Operations Dashboard, který byl implementován v tomto oboru názvů, pak je třeba Registrace s produktem Operations Dashboard.

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

Operator2.2.0 OpenShift CP4I Integrace produktu IBM MQ s trasováním IBM Instana

IBM Instana lze použít k trasování transakcí v rámci produktu IBM Cloud Pak for Integration.

Než začnete

Tento dokument pokrývá trasování systému IBM Instana , což je proces trasování zpráv prostřednictvím systému. Nepokrývá monitorování produktu IBM Instana , ve kterém jsou načítány podrobnosti o stavu správce front produktu IBM MQ . Informace týkající se monitorování produktu IBM MQ pomocí IBM Instana viz Monitorování IBM MQ. Podrobné pokyny k ověřenému monitorování viz “Konfigurace ověřeného monitorování produktu IBM Instana s protokolem TLS” na stránce 157.

Poznámka:

- Tuto funkci lze použít pouze s produktem IBM MQ Operator verze 2.2.0 a novější. Tato funkce je podporována pouze v operandech produktu IBM MQ verze 9.3.1.0-r2 nebo novější.
- Trasování IBM Instana můžete spustit na předchozích verzích produktu IBM MQ Operator a správce front, nikoli však nativně. Viz téma Konfigurace IBM MQ Trasování v dokumentaci k produktu IBM Instana .

Než budete moci provést trasování IBM Instana s operátorem IBM MQ , musíte implementovat agenty IBM Instana typu backend i IBM Instana . Správce front IBM MQ standardně komunikuje s agentem IBM Instana implementovaným ve stejném uzlu jako sekce správce front.

Informace o této úloze

Povolení integrace s produktem IBM Instana způsobí instalaci uživatelské procedury rozhraní API produktu IBM MQ ve vašem správci front. Uživatelská procedura rozhraní API odesílá data trasování do agentů IBM Instana o zprávách, které procházejí správcem front.

Uživatelská procedura rozhraní API přidá záhlaví RFH2 ke každé zprávě. Tato záhlaví obsahují informace o trasování.

Agenti IBM Instana jsou zodpovědní za odeslání dat trasování do back-endového systému IBM Instana .

Chcete-li získat informace o implementaci IBM Instana back-endových a IBM Instana agentů, prohlédněte si téma Povolení IBM Instana monitorování v CP4I Platform UI v dokumentaci k produktu IBM Instana .

Procedura

Standardní nasazení

- Implementujte správce front s povoleným trasováním IBM Instana .

  Standardně je trasování IBM Instana zakázáno.

  Pokud používáte webovou konzolu IBM Cloud Pak for Integration Platform UI (previously the Platform Navigator) nebo OpenShift :

1. Klepněte na volbu **Telemetrie** > **Trasování** > **Instana**.
2. Nastavte přepínač **Povolit trasování instance** na hodnotu `true`.

Pokud implementujete prostřednictvím YAML, použijte následující úsek kódu:

```
spec:
  telemetry:
    tracing:
      instana:
        enabled: true
```

Rozšířená implementace

- Komunikujte s agentem IBM Instana přes https.

  Standardně IBM Instana exit for IBM MQ komunikuje s agentem IBM Instana přes http. Adresa hostitele agenta je nastavena na adresu IP uzlu, na kterém je spuštěn správce front. Toto odpovídá konfiguraci popsané v části Povolení IBM Instana monitorování v dokumentaci IBM Instana , kde jsou agenti IBM Instana implementováni operátorem IBM Instana Agent Operator jako denní nástup.

  Momentálně komunikace mezi uživatelskou procedurou IBM Instana pro IBM MQ a agentem IBM Instana podporuje protokoly http nebo https. Chcete-li používat protokol https, musí být agent IBM Instana nejprve nakonfigurován pro použití šifrování TLS. Viz Nastavení šifrování TLS pro koncový bod agenta v dokumentaci IBM Instana . Protokol pak může být nastaven na https takto:

  Pokud používáte webovou konzolu OpenShift :

  1. Klepněte na volbu **Telemetrie** > **Instana**.
  2. Rozbalte rozevírací seznam **Rozšířená konfigurace** .
  3. Nastavte **Komunikační protokol agenta instance** na hodnotu `https`.

  Pokud implementujete prostřednictvím YAML, použijte následující úsek kódu:

  ```
  spec:
    telemetry:
      instana:
        enabled: true
        protocol: https
  ```

- Nastavení **`agentHost`**

  Pokud agenti IBM Instana nebyli implementováni jako démon v klastru Openshift, kde je spuštěn správce front, musíte nastavit hodnotu **`agentHost`** na název hostitele nebo adresu IP, kde je spuštěn agent IBM Instana . Hodnota **`agentHost`** by neměla obsahovat protokol nebo port.

  Pokud používáte webovou konzolu OpenShift :

  1. Klepněte na volbu **Telemetrie** > **Instana**.
  2. Rozbalte rozevírací seznam **Rozšířená konfigurace** .
  3. Zadejte název hostitele do textového pole **Instana agent host** .

  Pokud implementujete prostřednictvím YAML, použijte následující úsek kódu:

  ```
  spec:
    telemetry:
      instana:
        enabled: true
        agentHost: 9.9.9.9
  ```

Jak pokračovat dále

Další informace najdete v tématu “Implementace správce front do klastru Red Hat OpenShift Container Platform” na stránce 114.

Operator2.2.0 OpenShift CP4I

Konfigurace ověřeného monitorování produktu IBM Instana s protokolem TLS

Chcete-li mít možnost monitorovat správce front prostřednictvím agenta IBM Instana , musíte nakonfigurovat agenta i správce front.

Než začnete

Část "Konfigurace" produktu "Monitoring IBM MQ" v dokumentaci k produktu IBM Instana poskytuje obecné informace týkající se konfigurace monitorování produktu IBM Instana . Nezahrnuje však podrobnosti o konfiguraci správce front.

Než budete moci provést trasování IBM Instana s operátorem IBM MQ , musíte implementovat agenty IBM Instana typu backend i IBM Instana . Chcete-li to provést, prohlédněte si téma Povolení monitorování instance IBM v uživatelském rozhraní CP4I Platform UI v IBM Instana dokumentaci.

Postup

1. Generovat certifikáty.
2. Konfigurovat IBM Instana agenty.
3. Konfigurovat správce front.
4. Ověřit a ladit.

Související úlohy

“Integrace produktu IBM MQ s trasováním IBM Instana” na stránce 155
IBM Instana lze použít k trasování transakcí v rámci produktu IBM Cloud Pak for Integration.

Operator2.2.0 OpenShift CP4I

Generovat certifikát a klíč pro agenta IBM Instana a správce front

Pro komunikaci TLS mezi agentem IBM Instana a správcem front musí mít oba certifikát a odpovídající soukromý klíč.

Než začnete

Jedná se o první ze čtyř úloh konfigurace ověřeného IBM Instana monitorování pomocí TLS.

Poznámka: Hodnoty použité při generování těchto certifikátů jsou určeny pro demonstrační účely. Při implementaci v produkčním prostředí se ujistěte, že předmět a vypršení platnosti certifikátu jsou vhodné.

Postup

IBM MQ Správce front

Chcete-li komunikovat s agentem IBM Instana prostřednictvím protokolu TLS, musí mít správce front certifikát a odpovídající soukromý klíč. Pokud je již máte, přeskočte tuto sekci.

1. Vygenerujte certifikát a soukromý klíč pro správce front.

   Spusťte následující příkaz:

```
openssl req \
       -newkey rsa:2048 -nodes -keyout server.key \
       -subj "/CN=mq queuemanager/OU=ibm mq" \
       -x509 -days 3650 -out server.crt
```

IBM Instana agent

Má-li agent provádět komunikaci TLS se správcem front IBM MQ , musí mít certifikát a odpovídající soukromý klíč. Pokud již máte soukromý klíč a certifikát v úložišti klíčů JKS, který chcete použít, přeskočte tuto sekci.

2. Vygenerujte certifikát a soukromý klíč pro agenta IBM Instana .

Spusťte následující příkaz:

```
openssl req \
       -newkey rsa:2048 -nodes -keyout application.key \
       -subj "/CN=instana-agent/OU=app team1" \
       -x509 -days 3650 -out application.crt
```

3. Uložte certifikát a soukromý klíč do úložiště klíčů PKCS12 .

   Spusťte následující příkaz a nahraďte *vaše_heslo* heslem, které chcete použít k zabezpečení úložiště klíčů. Proveďte tuto náhradu ve všech následných krocích.

   ```
   openssl pkcs12 -export -out application.p12 -inkey application.key -in application.crt
   -passout pass:your_password
   ```

4. Převeďte úložiště klíčů PKCS12 na úložiště klíčů JKS.

   Spusťte následující příkaz:

   ```
   keytool -importkeystore \
           -srckeystore application.p12 \
           -srcstoretype pkcs12 \
           -destkeystore application.jks \
           -deststoretype JKS \
           -srcstorepass your_password \
           -deststorepass your_password \
           -noprompt
   ```

5. Popište certifikát.

   Spusťte následující příkaz:

   ```
   keytool -changealias -alias "1" -destalias "instana" -keypass your_password -keystore
   application.jks -storepass your_password -noprompt
   ```

6. Naimportujte certifikát správce front do úložiště klíčů.

   Spusťte následující příkaz:

   ```
   keytool -importcert -file server.crt -keystore application.jks -storepass your_password
   -alias myca -noprompt
   ```

Jak pokračovat dále

Nyní jste připraveni nakonfigurovat agenty pro IBM Instana monitorování.

Operator2.2.0 OpenShift CP4I

Monitorování instance: Konfigurace agentů

Připojte úložiště klíčů k agentům IBM Instana a poté nakonfigurujte monitorování pro specifického správce front.

Než začnete

Tato úloha předpokládá, že jste vygenerovali certifikát a klíč pro agenty IBM Instana a správce front.

Postup

Připojení úložiště klíčů k IBM Instana agentům

1. Vytvořte tajný klíč z úložiště klíčů JKS v oboru názvů agenta IBM Instana .

   Spusťte následující příkaz a nahraďte *keystore_secret_name* názvem, který chcete použít. Proveďte tuto náhradu ve všech následných krocích.

   ```
   oc create secret generic keystore_secret_name --from-file=./application.jks -n instana-agent
   ```

2. V oboru názvů instana-agent použijte příkaz `oc edit daemonset instana-agent` k úpravě démonového produktu instana-agent, aby zahrnoval následující přídavné volumeMount a svazek:

```
volumeMounts:
- name: mq-key-jks-name
   subPath: application.jks
   mountPath: /opt/instana/agent/etc/application.jks
volumes:
- name: mq-key-jks-name
   secret:
      secretName: keystore_secret_name
```

Konfigurace monitorování pro specifického správce front

3. V oboru názvů instana-agent použijte příkaz `oc edit configmap instana-agent` k úpravě configmap instana-agent.
4. Přidejte následující sekci pod `configuration.yaml: |`. Pokud jste již tuto sekci definovali, přidejte do seznamu nového správce front.

```
    com.instana.plugin.ibmmq:
      enabled: true
      poll_rate: 60
      queueManagers:
         QUEUE_MANAGER_NAME:
            channel: 'INSTANA.A.SVRCONN'
            keystorePassword: 'your_password'
            keystore: '/opt/instana/agent/etc/application.jks'
            cipherSuite: 'TLS_RSA_WITH_AES_256_CBC_SHA256'
```

   kde:

   - *vaše_heslo* je heslo k úložišti klíčů JKS.
   - *QUEUE_MANAGER_NAME* je název základního správce front IBM MQ , který má být implementován, a nikoli název operandy správce front.

   Poznámka: Není-li parametr *QUEUE_MANAGER_NAME* nastaven na základní název správce front a je nastaven na hodnotu Operand, monitorování nebude fungovat. Základní název je definován v souboru `spec.queuemanager.name` pro operátor správce front.
5. Odstraňte sekce instana-agent z oboru názvů instana-agent. To způsobí jejich restart a zahájení monitorování s novým nastavením.

Jak pokračovat dále

Nyní jste připraveni nakonfigurovat správce front pro IBM Instana monitorování.

Operator2.2.0 OpenShift CP4I

Monitorování instance: Konfigurace správce front

Nastavte správce front, který používá TLS ke komunikaci s agentem IBM Instana .Ověření pro toto připojení se provádí pomocí příkazu SSLPEERMAP.

Než začnete

Tato úloha předpokládá, že jste nakonfigurovali agenty pro IBM Instana monitorování.

Postup

1. Konfigurujte správce front prostřednictvím MQSC i INI.

   MQSC se používá k nastavení nového kanálu s povoleným zabezpečením TLS a poté se tento kanál konfiguruje pro ověření připojujícího se agenta IBM Instana , pokud má certifikát s požadovanými poli. V tomto případě namapujeme všechny připojující se klienty s certifikátem obsahujícím pole `CN=instana-agent,OU=app team1` na uživatele `app1`. MQSC pak udělí oprávnění uživateli `app1` provádět požadované operace pro monitorování produktu IBM Instana .

   Soubor INI se používá k udělení oprávnění našemu externímu uživateli `app1`.

   Následující konfigurační mapa obsahuje požadovaná nastavení MQSC a INI. Implementujte jej do oboru názvů správce front.

```
apiVersion: v1
data:
  channel.mqsc: |-
    DEFINE CHANNEL('INSTANA.A.SVRCONN') CHLTYPE(SVRCONN) SSLCAUTH(REQUIRED)
SSLCIPH('ANY_TLS12_OR_HIGHER')
    ALTER QMGR CONNAUTH(' ')
    REFRESH SECURITY
    SET CHLAUTH('INSTANA.A.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=*') USERSRC(NOACCESS)
ACTION(REPLACE)
    SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
    SET CHLAUTH('INSTANA.A.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=instana-agent,OU=app
team1') USERSRC(MAP) MCAUSER('app1')
    SET AUTHREC PRINCIPAL('app1') OBJTYPE(QMGR) AUTHADD(ALL)
    SET AUTHREC PROFILE('SYSTEM.ADMIN.COMMAND.QUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE)
AUTHADD(PUT,INQ,DSP,CHG)
    SET AUTHREC PROFILE('SYSTEM.**') PRINCIPAL('app1') OBJTYPE(TOPIC) AUTHADD(DSP)
    SET AUTHREC PROFILE('*') PRINCIPAL('app1') OBJTYPE(TOPIC) AUTHADD(DSP)
    SET AUTHREC PROFILE('SYSTEM.**') PRINCIPAL('app1') OBJTYPE(QUEUE) AUTHADD(DSP, CHG, GET)
    SET AUTHREC PROFILE('SYSTEM.**') PRINCIPAL('app1') OBJTYPE(LISTENER) AUTHADD(DSP)
    SET AUTHREC PROFILE('AMQ.*') PRINCIPAL('app1') OBJTYPE(QUEUE) AUTHADD(DSP, CHG)
    REFRESH SECURITY TYPE(CONNAUTH)
  auth.ini: |-
    Service:
      Name=AuthorizationService
      EntryPoints=14
      SecurityPolicy=UserExternal
kind: ConfigMap
metadata:
  namespace: your-queue-manager-namespace
  name: qmgr-monitoring-config
```

kde *your-queue-manager-namespace* je obor názvů, ve kterém bude implementován váš správce front.

Poznámka: Pokud monitorujete fronty definované uživatelem, musíte přidat další řádky do configmap MQSC, čímž těmto frontám udělíte oprávnění DSP, CHG a GET. Příklad:

```
SET AUTHREC PROFILE('MYQUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE) AUTHADD(DSP, CHG, GET).
```

Tento příklad používá configmap pro data MQSC a INI, ale můžete použít tajný klíč, pokud jsou vámi přidané údaje důvěrné. Obecné informace týkající se implementace s MQSC a INI naleznete v části “Příklad: Dodání souborů MQSC a INI” na stránce 133.

2. Aby bylo možné vytvořit připojení TLS, musí správce front důvěřovat certifikátu agenta IBM Instana . Chcete-li toho dosáhnout, vytvořte tajný klíč obsahující pouze certifikát agenta IBM Instana :

```
oc create secret generic instana-certificate-secret --from-file=./application.crt -n your-
queue-manager-namespace
```

3. Správce front musí předložit vlastní certifikát pro navázání komunikace TLS a vyžaduje přístup k přidruženému soukromému klíči. Nasaďte tajný klíč obsahující klíč a certifikát, který jste buď vytvořili dříve, nebo který již vlastníte:

```
oc create secret tls qm-tls-secret --cert server.crt --key server.key -n your-queue-manager-
namespace
```

S vytvořenou konfigurační mapou a tajným klíčem jste připraveni vytvořit samotného správce front.

4. Ujistěte se, že váš správce front YAML nenastavuje proměnnou prostředí **MQSNOAUT** v kontejneru správce front.

Jinak po povolení nebude mechanizmus ověřování fungovat. Odebrání proměnné po implementaci nezpůsobí opětovné povolení mechanizmu a je třeba znovu vytvořit správce front.

5. Do definice správce front přidejte následující sekce, kde *MYQM* je název vašeho správce front:

```
spec:
  queueManager:
    name: MYQM   #(a)
    ini:   #(b)
      - configMap:
          items:
            - auth.ini
          name: qmgr-monitoring-config
```

```
    mqsc:   #(c)
      - configMap:
          items:
            - channel.mqsc
          name: qmgr-monitoring-config
  pki:
    keys:   #(d)
        - name: default
          secret:
            items:
            - tls.key
            - tls.crt
            secretName: qm-tls-secret
    trust:   #(e)
      - name: app
        secret:
          items:
            - application.crt
          secretName: instana-certificate-secret
```

Označené sekce specifikace jsou popsány takto:

a. Ujistěte se, že jste svému základnímu správci front dali jedinečný název. Pokud základní správce front nemá jedinečný název, nemusí monitorování fungovat tak, jak bylo zamýšleno. Tento název se musí shodovat s názvem v souboru configmap agenta IBM Instana , který byl dříve upraven.

b. Informace INI zapsané do mapy configmap jsou přidány do správce front.

c. Informace MQSC, které byly zapsány do mapy configmap, jsou přidány do správce front.

d. Certifikát správce front a soukromý klíč jsou přidány do úložiště klíčů správce front.

e. Certifikát agenta IBM Instana je přidán do úložiště údajů o důvěryhodnosti správce front.

6. Volitelné: Povolte trasování IBM Instana v monitorovaném správci front.

   Chcete-li to provést, viz “Integrace produktu IBM MQ s trasováním IBM Instana” na stránce 155.

7. Implementujte správce front.

Jak pokračovat dále

Nyní jste připraveni ověřit a ladit IBM Instana monitorování.

Operator2.2.0 OpenShift CP4I

Monitorování instance: Ověření a ladění

Chcete-li mít možnost monitorovat správce front prostřednictvím agenta IBM Instana , musíte nakonfigurovat agenta i správce front.

Než začnete

Tato úloha předpokládá, že jste nakonfigurovali správce front pro IBM Instana monitorování.

Postup

ověření

1. Chcete-li ověřit, zda byla implementace úspěšná, zobrazte svého správce front v panelu dashboard produktu IBM Instana .

   Správce front by měl být viditelný v sekci služeb na stránce aplikace a také v pohledu Infrastruktura.

Ladění

Poznámka: Tyto kroky ladění předpokládají implementaci Openshift agenta IBM Instana spuštěného jako démon.

Pokud nevidíte svého správce front v panelu dashboard produktu IBM Instana , možná jste nesprávně nakonfigurovali svého správce front. Chcete-li provést vyšetření, postupujte takto.

2. Identifikujte uzel, na kterém je aktivní sekce správce front spuštěna.

   Spusťte následující příkaz v oboru názvů správce front:

```
oc get pods -o wide -n your-queue-manager-namespace
```

3. Chcete-li určit, která sekce agenta IBM Instana je spuštěna ve stejném uzlu jako správce front, spusťte stejný příkaz v oboru názvů instana-agent:

```
oc get pods -o wide -n instana-agent-namespace
```

4. Chcete-li lépe porozumět problémům na straně agenta IBM Instana , získejte protokoly sekce agenta IBM Instana a vyhledejte položky týkající se 'mq' nebo názvu vašeho správce front.

   Spusťte následující příkaz:

```
oc logs instana-agent-pod -c instana-agent -n instana-agent
```

5. Zkontrolujte protokoly správce front.

   Pokud se agent pokusil o připojení ke správci front, měly by protokoly správce front indikovat, proč připojení nebylo úspěšné. Spusťte následující příkaz:

```
oc logs your-queue-manager-name -n your-queue-manager-namespace
```

Výsledky

Dokončili jste všechny čtyři úlohy pro konfiguraci ověřeného IBM Instana monitorování pomocí TLS.

OpenShift CP4I Sestavení obrazu pomocí vlastních souborů MQSC a INI s použitím rozhraní CLI Red Hat OpenShift

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 Red Hat OpenShift Container Platform rozhraní příkazového řádku.

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

Pokud nemáte tajný klíč Red Hat OpenShift pro registr IBM Entitled Registry ve vašem projektu Red Hat OpenShift , postupujte podle kroků pro volbu Vytvořit tajný klíč nároku.

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:9.3.5.1-r2
      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:9.3.5.1-r2"
      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 (podrobnosti viz “Historie vydání pro IBM MQ Operator” na stránce 34). 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 do klastru Red Hat OpenShift Container Platform” na stránce 114 a přidejte nový vlastní obraz do YAML.

Do svého běžného YAML produktu `QueueManager` můžete přidat následující úsek YAML, kde *můj obor názvů* je projekt/obor názvů produktu Red Hat OpenShift, který používáte, a *obraz* je název obrazu, který jste vytvořili dříve (například "mymq:latest-amd64"):

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

Související úlohy

“Implementace správce front do klastru Red Hat OpenShift Container Platform” na stránce 114

Tento příklad implementuje správce front "rychlého spuštění", který používá dočasné (dočasné) úložiště a vypíná zabezpečení produktu IBM MQ . Zprávy nejsou trvale uchovávány při restartování správce front. Konfiguraci můžete upravit tak, aby bylo možné změnit mnoho nastavení správce front.

OpenShift CP4I Přidání vlastních anotací a štítků do prostředků správce front

Do metadat správce front můžete přidávat vlastní anotace a štítky.

Informace o této úloze

Vlastní anotace a štítky jsou přidány ke všem prostředkům s výjimkou PVC. Jestliže se vlastní anotace nebo štítek shoduje s existujícím klíčem, použije se hodnota nastavená pomocí IBM MQ Operator.

Procedura

- Přidejte vlastní anotace.

  Chcete-li přidat vlastní anotace do prostředků správce front, včetně podu, přidejte anotace pod `metadata`. Příklad:

  ```
  apiVersion: mq.ibm.com/v1beta1
  kind: QueueManager
  metadata:
    name: quickstart-cp4i
    annotations:
      annotationKey: "value"
  ```

- Přidat vlastní štítky.

  Chcete-li přidat vlastní štítky do prostředků správce front, včetně podu, přidejte štítky pod `metadata`. Příklad:

  ```
  apiVersion: mq.ibm.com/v1beta1
  kind: QueueManager
  metadata:
    name: quickstart-cp4i
    labels:
      labelKey: "value"
  ```

OpenShift CP4I Zakázání běhových kontrol webhooku

Běhové kontroly webohooku zajišťují, že paměťové třídy jsou pro správce front životaschopné. Zakážete je pro zlepšení výkonu nebo protože nejsou platné pro vaše prostředí.

Informace o této úloze

Běhové kontroly webohooku jsou prováděny v konfiguraci správce front. Kontrolujete, zda jsou paměťové třídy vhodné pro vybraný typ správce front.

Můžete se rozhodnout zakázat tyto kontroly kvůli zkrácení doby potřebné pro vytvoření správce front, nebo kvůli tomu, že tyto kontroly nejsou platné pro vaše specifické prostředí.

Poznámka: Po zakázání běhových kontrol webhooku jsou povoleny všechny hodnoty paměťové třídy. V důsledku toho může dojít k poškození správce front.

Procedura

- Zakažte běhové kontroly webhooku.

  Přidejte následující anotaci pod `metadata`. Příklad:

  ```
  apiVersion: mq.ibm.com/v1beta1
  kind: QueueManager
  ```

```
metadata:
  name: quickstart-cp4i
  annotations:
    "com.ibm.cp4i/disable-webhook-runtime-checks" : "true"
```

OpenShift Operator 2.1.0 CP4I Zakázání aktualizací výchozích hodnot pro specifikaci správce front

Produkt IBM MQ Operator aktualizuje všechny nespecifikované hodnoty ve specifikaci správce front pomocí jejich výchozích hodnot. Chcete-li se vyhnout úpravám specifikace správce front, můžete toto chování zakázat. Pole stavu správce front jsou stále aktualizována.

Procedura

- Zakázat aktualizace výchozích hodnot správce front.

  Přidejte následující anotaci pod `metadata`. Příklad:

  ```
  apiVersion: mq.ibm.com/v1beta1
  kind: QueueManager
  metadata:
    name: quickstart-cp4i
    annotations:
      "com.ibm.mq/write-defaults-spec" : "false"
  ```

  Poznámka: Tuto funkci lze použít pouze s operátorem MQ 2.1.0 a novějšími verzemi. Od verze IBM MQ Operator 2.1.0mají příklady rychlého spuštění standardně použitou tuto anotaci.

V 9.3.4 Spuštění kontejneru IBM MQ s kořenovým systémem souborů jen pro čtení

V produktu IBM MQ Operator 3.0.0 a IBM MQ kontejner 9.3.4.0můžete nakonfigurovat kontejner IBM MQ tak, aby byl spuštěn s kořenovým systémem souborů jen pro čtení. To zabraňuje útočníkům v kopírování a spouštění škodlivého kódu v kontejneru.

Informace o této úloze

Povolením kořenového systému souborů jen pro čtení se soubory kontejneru stane neměnné. To znamená, že v systému souborů kontejneru lze soubory prohlížet, ale nelze je upravovat a nelze vytvářet žádné nové soubory. Soubory lze upravit nebo vytvořit pouze v připojeném systému souborů.

Když je povolen kořenový systém souborů jen pro čtení, vytvoří se dva dočasné svazky `Scratch` a `Tmp` a připojí se v adresářích `/run` a `/tmp` v kontejneru.

- Svazek `Scratch` obsahuje soubory, úložiště klíčů a další soubory používané pro konfiguraci správce front.
- Svazek `Tmp` obsahuje diagnostické soubory, například soubory RAS správce front.

Protože jsou tyto svazky pomíjivé, soubory na těchto svazcích se při restartu pod ztratí.

Typ svazku vytvořeného pro data správce front závisí na typu úložiště. Standardně je připojen trvalý svazek. Nebo je-li typ úložiště `efemérní`, je připojen efemérní svazek. Pokud velikost dat ve svazku překročí hodnotu zadanou pro vlastnost **`sizeLimit`** , pak může produkt Kubernetes vysunout kontejner a vytvořit nový. Před verzí IBM MQ Operator 3.0.0nebyl vynucen limit velikosti při použití přechodného úložiště pro data správce front.

Kořenový systém souborů jen pro čtení není standardně povolen. Chcete-li jej povolit, postupujte takto:

Postup

1. Pomocí rozhraní API `spec.securityContext` povolte kořenový systém souborů jen pro čtení.

Pro svého správce front nastavte vlastnost **readOnlyRootFilesystem** v souboru ".spec.securityContext" na stránce 192 na hodnotu `true`.

Produkt IBM MQ Operator vytvoří dva dočasné svazky `Scratch` a `Tmp`.

2. Volitelné: Nastavte nebo změňte typ datového úložiště správce front.

   Standardně je nárok na trvalý svazek připojen na adrese `/mnt/mqm`. Nebo je-li vlastnost **type** v souboru ".spec.queueManager.storage.queueManager" na stránce 190nastavena na hodnotu `efemérní` , vytvoří se a připojí se efemérní svazek.
3. Pro každý pomíjivý objem pečlivě zvažte, o kolik by data mohla růst. Nastavte odpovídajícím způsobem hodnotu vlastnosti **sizeLimit** , včetně jednotek SI.
   - Pro dočasný svazek `Scratch` nastavte vlastnost **sizeLimit** v souboru ".spec.queueManager.storage.scratch" na stránce 192. Výchozí hodnota je "100M".
   - Pro dočasný svazek `Tmp` nastavte vlastnost **sizeLimit** v souboru ".spec.queueManager.storage.tmp" na stránce 192. Výchozí hodnota je "2Gi".
   - Je-li parametr **type** svazku správce front nastaven na hodnotu `efemeral`, nastavte vlastnost **sizeLimit** v souboru ".spec.queueManager.storage.queueManager" na stránce 190. Výchozí hodnota je "2Gi".

OpenShift V 9.3.4 Konfigurace konzoly IBM MQ Console se základním registrem pomocí konzoly IBM MQ Operator

Chcete-li se přihlásit k produktu IBM MQ Console, můžete správci front dodat vlastní konfiguraci.

Než začnete

Pokud implementujete správce front s licencí IBM MQ Advanced for Developers , je zde vestavěná jednoduchá konfigurace. Viz téma "[MQ 9.3.4 Pro 2023]Příklad správce front YAML, který popisuje, jak zadat hesla pro admin a app uživatele" na stránce 24.

Pokud implementujete správce front licencí IBM Cloud Pak for Integration , můžete povolit integraci s produktem IBM Cloud Pak for Integration Keycloak pro přihlášení k produktu IBM MQ Console pomocí jednotného přihlášení. Viz téma "Připojení k serveru IBM MQ Console implementovanému v Red Hat OpenShift" na stránce 168.

Postup

1. **Vytvořte heslo a zašifrujte jej pomocí `securityUtility`.**

   `ConfigMap` se používá k uložení pověření, která používáte pro přístup ke správci front. Chcete-li zlepšit zabezpečení, zakódujte tato pověření pomocí příkazu securityUtility.

   Alternativně můžete použít tajný klíč, který chrání pověření ve vrstvě Kubernetes . Nástroje pro monitorování a odstraňování problémů však mohou základní soubor vystavit nezabezpečeně.
2. Volitelné: **Přihlaste se do rozhraní příkazového řádku (CLI) Red Hat OpenShift .**

   Pokud používáte rozhraní příkazového řádku OpenShift , přihlaste se pomocí `oc login`.

   Případně můžete použít konzolu OpenShift .
3. **Vytvořte soubor `ConfigMap` se svou konfigurací.**

   Nápovědu k vytvoření konfigurace XML naleznete v části IBM MQ Console a REST API zabezpečení.

   Následující příklad vytvoří uživatele ve skupině `MQWebAdminGroup`. Členům skupiny `MQWebAdminGroup` je přiřazena role `MQWebAdmin` . V tomto příkladu platí následující:

   - **Musíte** nahradit hodnoty *USERNAME* a *PASSWORD* svými vlastními hodnotami. Všimněte si, že *USERNAME* se v příkladu používá dvakrát.

     Musíte určit *NAMESPACE* jako ten, ve kterém je implementován produkt IBM MQ Operator a kde bude nebo již bude implementován váš správce front.

a) Pomocí konzoly OpenShift nebo příkazového řádku vytvořte následující ConfigMap:

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: mqwebuserconfigmap
  namespace: NAMESPACE
data:
  mqwebuser.xml: |
    <?xml version="1.0" encoding="UTF-8"?>
    <server>
      <featureManager>
        <feature>appSecurity-2.0</feature>
        <feature>basicAuthenticationMQ-1.0</feature>
      </featureManager>
      <enterpriseApplication id="com.ibm.mq.console">
        <application-bnd>
          <security-role name="MQWebAdmin">
            <group name="MQWebAdminGroup" realm="defaultRealm"/>
          </security-role>
        </application-bnd>
      </enterpriseApplication>
      <basicRegistry id="basic" realm="defaultRealm">
        <user name="USERNAME" password="PASSWORD"/>
        <group name="MQWebAdminGroup">
          <member name="USERNAME"/>
        </group>
      </basicRegistry>
      <sslDefault sslRef="mqDefaultSSLConfig"/>
    </server>
```

b) Volitelné: Používáte-li příkazový řádek, použijte příkaz ConfigMap:

```
oc apply -f mqwebuserconfigmap.yaml
```

Pro zbývající kroky vyberte jednu z následujících voleb:

- Implementujte nového správce front s konfigurací pro přístup k souboru IBM MQ Console.
- Použijte konfiguraci, která poskytuje produktu IBM MQ Console přístup k existujícímu správci front.

4. Volitelné: **Implementujte nového správce front s konfigurací pro přístup k serveru IBM MQ Console.**

a) Vytvořte správce front.

Nastavte poskytovatele ověření a autorizace na ručnía dodejte nově vytvořený produkt ConfigMap mqwebuserconfigmap pomocí jedné z následujících voleb:

- Volba 1: Prostřednictvím správce front YAML

  Přidejte následující kód do sekce web správce front YAML:

```
...
web:
    enabled: true
    console:
      authentication:
        provider: manual
      authorization:
        provider: manual
    manualConfig:
      configMap:
        name: mqwebuserconfigmap
```

- Volba 2: Prostřednictvím pohledu Formulář konzoly OpenShift :

  i) V konzole OpenShift vyberte volbu **Operátory** > **Instalované operátory**.

  ii) Vyberte implementaci produktu IBM MQ Operator.

  iii) Vyberte volbu **Správce front** a klepněte na volbu **Vytvořit QueueManager**.

  iv) Vyberte příslušné volby pro správce front.

  v) Vyberte volbu **Web** a nastavte volbu **Povolit webový server** na hodnotu true.

  vi) Otevřete okénko se seznamem **Rozšířená konfigurace** .

vii) V okénku se seznamem **Konzola** nastavte **poskytovatele** pro **Ověření** i **Autorizace** na `ruční`.

viii) Otevřete okénko se seznamem **Konfigurace** .

ix) Otevřete okénko se seznamem **ConfigMap** a vyberte volbu ConfigMap `mqwebuserconfigmap` , která byla vytvořena v kroku “3” na stránce 166.

x) Klepněte na volbu **Vytvořit**.

Nyní můžete přistupovat k produktu IBM MQ Console vašeho nového správce front prostřednictvím pověření uvedených v části `ConfigMap` vytvořené v kroku “3” na stránce 166.

5. Volitelné: **Použít konfiguraci, která povoluje IBM MQ Console pro existujícího správce front.**

   Upravte YAML správce front, pro kterého povolujete IBM MQ Console:

   a. V konzole OpenShift vyberte volbu **Operátory** > **Instalované operátory**.

   b. Vyberte implementaci produktu IBM MQ Operator.

   c. Vyberte volbu **Správce front** a vyberte název správce front.

   d. Vyberte volbu **YAML**.

   e. Nahraďte existující sekci web správce front YAML následujícím kódem:

```
...
web:
    enabled: true
    console:
      authentication:
        provider: manual
      authorization:
        provider: manual
    manualConfig:
      configMap:
        name: mqwebuserconfigmap
```

   f. Klepněte na tlačítko **Uložit**.

   Nyní můžete přistupovat k produktu IBM MQ Console existujícího správce front prostřednictvím pověření uvedených v `ConfigMap` vytvořeném v kroku “3” na stránce 166.

OpenShift CP4I Provozování produktu IBM MQ pomocí IBM MQ Operator

Procedura

- “Připojení k serveru IBM MQ Console implementovanému v Red Hat OpenShift” na stránce 168.
- “Monitorování při použití produktu IBM MQ Operator” na stránce 170.
- “Zálohování a obnova konfigurace správce front pomocí rozhraní Red Hat OpenShift CLI” na stránce 175.

OpenShift CP4I Připojení k serveru IBM MQ Console implementovanému v Red Hat OpenShift

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

Informace o této úloze

Adresu URL IBM MQ Console lze nalézt na stránce s podrobnostmi `QueueManager` ve webové konzole Red Hat OpenShift nebo v souboru IBM Cloud Pak for Integration Platform UI (previously the Platform

Navigator). Eventuálně je možné jej nalézt z rozhraní CLI Red Hat OpenShift spuštěním následujícího příkazu:

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

Pokud používáte licenci IBM Cloud Pak for Integration :

- Pro produkt IBM MQ Operator 3.0.0 a novější produkt IBM MQ Console používá Keycloak pro správu identit a přístupů. Viz Správa identit a přístupů v dokumentaci k produktu IBM Cloud Pak for Integration .
- Pro implementace systému IBM MQ Operator starší než verze 3.0.0používá produkt IBM MQ Console modul IBM Cloud Pak Identity and Access Manager (IAM). Komponenta IAM již mohla být nastavena administrátorem klastru. Pokud se však jedná o první použití IAM ve vašem klastru Red Hat OpenShift , musíte načíst počáteční heslo administrátora. Viz Získání počátečního hesla administrátora.

Pokud používáte licenci na produkt IBM MQ , pak produkt IBM MQ Console není předkonfigurovaný a musíte jej nakonfigurovat sami. Další informace viz Konfigurace uživatelů a rolí. Příklad viz “Konfigurace konzoly IBM MQ Console se základním registrem pomocí konzoly IBM MQ Operator” na stránce 166.

Související úlohy

“Konfigurace trasy pro připojení ke správci front mimo klastr Red Hat OpenShift” na stránce 152
Chcete-li připojit aplikaci ke správci front IBM MQ mimo klastr Red Hat OpenShift , potřebujete trasu Red Hat OpenShift . Musíte povolit TLS ve svém správci front IBM MQ a klientské aplikaci, protože SNI je k dispozici pouze v protokolu TLS, když se používá protokol TLS 1.2 nebo vyšší. Red Hat OpenShift Container Platform Router používá SNI ke směrování požadavků na správce front IBM MQ.

OpenShift CP4I *Udělení oprávnění pro IBM MQ Console pomocí modulu IBM Cloud Pak IAM*

Oprávnění pro produkt IBM MQ Console jsou spravována prostřednictvím produktu IBM Cloud Pak Administration Hub, a nikoli prostřednictvím produktu IBM Cloud Pak for Integration Platform UI (previously the Platform Navigator). Produkt IBM MQ nepoužívá oprávnění "Automatizace" poskytnutá produktem IBM Cloud Pak for Integration, ale místo toho používá základní oprávnění povolená produktem IBM Cloud Pak Identity and Access Manager (IAM).

Postup

1. Otevřete administrativní konzolu IBM Cloud Pak .

   V produktu IBM Cloud Pak for Integration Platform UIklepněte na přepínač Cloud Pak (9bodová ikona) v pravém horním rohu panelu nástrojů a pak klepněte na panel **IBM Cloud Pak Administration** .
2. V navigační nabídce v levém horním rohu vyberte volbu **Identita a přístup**a poté vyberte volbu **ID týmů a služeb**.
3. Vytvořte tým a poté do něj přidejte uživatele.
   a) Vyberte volbu **Vytvořit tým**.
   b) Zadejte název týmu a poté vyberte doménu zabezpečení pro uživatele, které chcete spravovat.
   c) Vyhledejte uživatele.

      Tito uživatelé již musí existovat ve vašem poskytovateli identit.
   d) Když najdete každého uživatele, dejte mu roli. Musíte mít hodnotu "Administrátor" nebo "Administrátor klastrů", chcete-li spravovat produkt IBM MQ pomocí konzoly IBM MQ Console.
4. Přidejte každého uživatele do prostoru jmen.
   a) Vyberte tým, který chcete upravit.
   b) Vyberte volbu **Prostředky** > **Spravovat prostředky**.
   c) Vyberte obory názvů, které má tento tým spravovat. Může se jednat o libovolné obory názvů se správcem front.

OpenShift CP4I Monitorování při použití produktu IBM MQ Operator

Správci front spravovaní produktem IBM MQ Operator mohou produkovat metriky kompatibilní s Prometheus.

Tyto metriky můžete zobrazit pomocí zásobníku monitorování Red Hat OpenShift Container Platform (OCP). Otevřete kartu **Metriky** v souboru OCPa poté klepněte na volbu **Sledovat** > **Metriky**. Metriky správce front jsou standardně povoleny, ale lze je zakázat nastavením **`.spec.metrics.enabled`** na hodnotu `false`.

Prometheus je databáze časových řad a generátor vyhodnocení pravidla pro metriky. Kontejnery produktu IBM MQ vystavují koncový bod metrik, na který se může dotazovat Prometheus. Metriky jsou generovány z témat systému MQ pro monitorování a trasování aktivity.

OpenShift Container Platform zahrnuje předkonfigurovaný, předinstalovaný zásobník a zásobník monitorování samoobslužné aktualizace používající server Prometheus. Zásobník monitorování OpenShift Container Platform je třeba konfigurovat pro monitorování uživatelem definovaných projektů. Další informace viz Povolení monitorování pro uživatelem definované projekty. IBM MQ Operator vytvoří `ServiceMonitor`, když vytvoříte `QueueManager` s povolenými metrikami, které pak může operátor Prometheus zjistit.

Ve starších verzích IBM Cloud Pak for Integration je možné také místo toho použít službu Monitorování platformy IBM Cloud k poskytnutí serveru Prometheus.

OpenShift CP4I *Metriky publikované při použití produktu IBM MQ Operator*

Kontejnery správce front mohou publikovat metriky kompatibilní s Red Hat OpenShift Monitoring.

Metric	Typ	Popis
`ibmmq_qmgr_commit_total`	`counter`	Počet potvrzení
`ibmmq_qmgr_cpu_load_fifteen_minute_average_percentage`	`gauge`	Zatížení procesoru - průměr za patnáct minut
`ibmmq_qmgr_cpu_load_five_minute_average_percentage`	`gauge`	Zatížení procesoru - průměr za pět minut
`ibmmq_qmgr_cpu_load_one_minute_average_percentage`	`gauge`	Zatížení procesoru - průměr za jednu minutu
`ibmmq_qmgr_destructive_get_bytes_total`	`counter`	Celkový počet bajtů destruktivních operací get pro interval
`ibmmq_qmgr_destructive_get_total`	`counter`	Celkový počet destruktivních operací get pro interval
`ibmmq_qmgr_durable_subscription_alter_total`	`counter`	Počet změn trvalého odběru
`ibmmq_qmgr_durable_subscription_create_total`	`counter`	Počet vytvoření trvalého odběru
`ibmmq_qmgr_durable_subscription_delete_total`	`counter`	Počet odstranění trvalého odběru

Metric	Typ	Popis
ibmmq_qmgr_durable_subscription_resume_total	counter	Počet obnovení trvalého odběru
ibmmq_qmgr_errors_file_system_free_space_percentage	gauge	Systém souborů chyb MQ - volné místo
ibmmq_qmgr_errors_file_system_in_use_bytes	gauge	Systém souborů chyb MQ - počet používaných bajtů
ibmmq_qmgr_expired_message_total	counter	Počet zpráv s vypršenou platností
ibmmq_qmgr_failed_browse_total	counter	Počet nezdařených procházení
ibmmq_qmgr_failed_mqcb_total	counter	Počet nezdařených operací MQCB
ibmmq_qmgr_failed_mqclose_total	counter	Počet nezdařených operací MQCLOSE
ibmmq_qmgr_failed_mqconn_mqconnx_total	counter	Počet nezdařených operací MQCONN/MQCONNX
ibmmq_qmgr_failed_mqget_total	counter	Počet nezdařených operací MQGET
ibmmq_qmgr_failed_mqinq_total	counter	Počet nezdařených operací MQINQ
ibmmq_qmgr_failed_mqopen_total	counter	Počet nezdařených operací MQOPEN
ibmmq_qmgr_failed_mqput1_total	counter	Počet nezdařených operací MQPUT1
ibmmq_qmgr_failed_mqput_total	counter	Počet nezdařených operací MQPUT
ibmmq_qmgr_failed_mqset_total	counter	Počet nezdařených operací MQSET
ibmmq_qmgr_failed_mqsubrq_total	counter	Počet nezdařených operací MQSUBRQ
ibmmq_qmgr_failed_subscription_create_alter_resume_total	counter	Počet nezdařených vytvoření/změn/obnovení odběru
ibmmq_qmgr_failed_subscription_delete_total	counter	Počet nezdařených odstranění odběru
ibmmq_qmgr_failed_topic_mqput_mqput1_total	counter	Počet nezdařených operací MQPUT/MQPUT1 tématu

Metric	Typ	Popis
ibmmq_qmgr_fdc_files	gauge	Počet souborů FDC MQ
ibmmq_qmgr_log_file_system_in_use_bytes	gauge	Systém souborů protokolu - počet používaných bajtů
ibmmq_qmgr_log_file_system_max_bytes	gauge	Systém souborů protokolu - maximální počet bajtů
ibmmq_qmgr_log_in_use_bytes	gauge	Protokol - počet používaných bajtů
ibmmq_qmgr_log_logical_written_bytes_total	counter	Protokol - počet logicky zapsaných bajtů
ibmmq_qmgr_log_max_bytes	gauge	Protokol - maximální počet bajtů
ibmmq_qmgr_log_occupied_by_reusable_extents_bytes	gauge	Protokol - bajty obsazené znovupoužitelnými oblastmi
ibmmq_qmgr_log_physical_written_bytes_total	counter	Protokol - počet fyzicky zapsaných bajtů
ibmmq_qmgr_log_primary_space_in_use_percentage	gauge	Protokol - aktuální používaný primární prostor
ibmmq_qmgr_log_required_for_media_recovery_bytes	gauge	Protokol - bajty nezbytné pro obnovení média
ibmmq_qmgr_log_workload_primary_space_utilization_percentage	gauge	Protokol - využití primárního prostoru pracovní zátěže
ibmmq_qmgr_log_write_latency_seconds	gauge	Protokol - latence zápisu
ibmmq_qmgr_log_write_size_bytes	gauge	Protokol - velikost zápisu
ibmmq_qmgr_mqcb_total	counter	Počet operací MQCB
ibmmq_qmgr_mqclose_total	counter	Počet operací MQCLOSE
ibmmq_qmgr_mqconn_mqconnx_total	counter	Počet operací MQCONN/MQCONNX
ibmmq_qmgr_mqctl_total	counter	Počet operací MQCTL
ibmmq_qmgr_mqdisc_total	counter	Počet operací MQDISC

Metric	Typ	Popis
ibmmq_qmgr_mqinq_total	counter	Počet operací MQINQ
ibmmq_qmgr_mqopen_total	counter	Počet operací MQOPEN
ibmmq_qmgr_mqput_mqput1_bytes_total	counter	Celkový počet bajtů operací MQPUT/MQPUT1 pro interval
ibmmq_qmgr_mqput_mqput1_total	counter	Celkový počet operací MQPUT/MQPUT1 pro interval
ibmmq_qmgr_mqset_total	counter	Počet operací MQSET
ibmmq_qmgr_mqstat_total	counter	Počet operací MQSTAT
ibmmq_qmgr_mqsubrq_total	counter	Počet operací MQSUBRQ
ibmmq_qmgr_non_durable_subscription_create_total	counter	Počet vytvoření dočasného odběru
ibmmq_qmgr_non_durable_subscription_delete_total	counter	Počet odstranění dočasného odběru
ibmmq_qmgr_non_persistent_message_browse_bytes_total	counter	Počet bajtů procházení dočasných zpráv
ibmmq_qmgr_non_persistent_message_browse_total	counter	Počet procházení dočasných zpráv
ibmmq_qmgr_non_persistent_message_destructive_get_total	counter	Počet dočasných zpráv destruktivních operací get
ibmmq_qmgr_non_persistent_message_get_bytes_total	counter	Počet bajtů získaných dočasných zpráv
ibmmq_qmgr_non_persistent_message_mqput1_total	counter	Počet dočasných zpráv operací MQPUT1
ibmmq_qmgr_non_persistent_message_mqput_total	counter	Počet dočasných zpráv operací MQPUT
ibmmq_qmgr_non_persistent_message_put_bytes_total	counter	Vložení dočasných zpráv - počet bajtů
ibmmq_qmgr_non_persistent_topic_mqput_mqput1_total	counter	Dočasné - počet operací MQPUT/MQPUT1 tématu

Metric	Typ	Popis
ibmmq_qmgr_persistent_message_browse_bytes_total	counter	Počet bajtů procházení trvalých zpráv
ibmmq_qmgr_persistent_message_browse_total	counter	Počet procházení trvalých zpráv
ibmmq_qmgr_persistent_message_destructive_get_total	counter	Počet trvalých zpráv destruktivních operací get
ibmmq_qmgr_persistent_message_get_bytes_total	counter	Počet bajtů získaných trvalých zpráv
ibmmq_qmgr_persistent_message_mqput1_total	counter	Počet trvalých zpráv operací MQPUT1
ibmmq_qmgr_persistent_message_mqput_total	counter	Počet trvalých zpráv operací MQPUT
ibmmq_qmgr_persistent_message_put_bytes_total	counter	Vložení trvalých zpráv - počet bajtů
ibmmq_qmgr_persistent_topic_mqput_mqput1_total	counter	Trvalé - počet operací MQPUT/MQPUT1 tématu
ibmmq_qmgr_published_to_subscribers_bytes_total	counter	Publikování odběratelům - počet bajtů
ibmmq_qmgr_published_to_subscribers_message_total	counter	Publikování odběratelům - počet zpráv
ibmmq_qmgr_purged_queue_total	counter	Počet vyprázdnění fronty
ibmmq_qmgr_queue_manager_file_system_free_space_percentage	gauge	Systém souborů správce front - volné místo
ibmmq_qmgr_queue_manager_file_system_in_use_bytes	gauge	Systém souborů správce front - počet používaných bajtů
ibmmq_qmgr_ram_free_percentage	gauge	Procentní část volné paměti RAM
ibmmq_qmgr_ram_usage_estimate_for_queue_manager_bytes	gauge	Celkový počet bajtů paměti RAM - odhad pro správce front
ibmmq_qmgr_rollback_total	counter	Počet odvolání

Metric	Typ	Popis
ibmmq_qmgr_system_cpu_time_estimate_for_queue_manager_percentage	gauge	Systémový čas procesoru - odhad procentní části pro správce front
ibmmq_qmgr_system_cpu_time_percentage	gauge	Procentní část systémového času procesoru
ibmmq_qmgr_topic_mqput_mqput1_total	counter	Celkový počet operací MQPUT/MQPUT1 tématu pro interval
ibmmq_qmgr_topic_put_bytes_total	counter	Celkový počet vložených bajtů tématu pro interval
ibmmq_qmgr_trace_file_system_free_space_percentage	gauge	Systém souborů trasování MQ - volné místo
ibmmq_qmgr_trace_file_system_in_use_bytes	gauge	Systém souborů trasování MQ - počet používaných bajtů
ibmmq_qmgr_user_cpu_time_estimate_for_queue_manager_percentage	gauge	Uživatelský čas procesoru - odhad procentní části pro správce front
ibmmq_qmgr_user_cpu_time_percentage	gauge	Procentní část uživatelského času procesoru

Související informace

Metriky publikované v tématech systému

OpenShift CP4I Zálohování a obnova konfigurace správce front pomocí rozhraní Red Hat 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.
  Můžete například spustit následující příkaz, kde *název_správce_front* je název vašeho prostředku `QueueManager`:

  ```
  oc get pods --selector app.kubernetes.io/name=ibm-mq,app.kubernetes.io/
  instance=queue_manager_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.
Můžete například spustit následující příkaz, kde *název_správce_front* je název vašeho prostředku `QueueManager`:

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

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

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

OpenShift CP4I Odstraňování problémů s produktem IBM MQ Operator

Pokud máte problémy s produktem IBM MQ Operator, mohou vám zde popsané metody pomoci při jejich diagnostice a řešení.

Procedura

- “Shromažďování informací o odstraňování problémů pro správce front implementované pomocí konzoly IBM MQ Operator” na stránce 176
- “Odstraňování problémů: Získání přístupu k datům správce front” na stránce 178

OpenShift CP4I Shromažďování informací o odstraňování problémů pro správce front implementované pomocí konzoly IBM MQ Operator

Shromažďování informací o odstraňování problémů, které by měly být poskytnuty podpoře IBM při vytváření nového případu podpory.

Postup

1. Shromážděte informace o poskytovateli cloudu.

   Jedná se o poskytovatele cloudu, který hostuje klastr Red Hat OpenShift (například IBM Cloud).
2. Shromážděte informace o architektuře.

   Architektura vašeho klastru Red Hat OpenShift je jedna z následujících:

   - Linux for x86-64
   - Linux on Power Systems (ppc64le)
   - Linux for IBM Z
3. Shromážděte informace o implementaci produktu IBM MQ .

   a) Přihlaste se ke svému klastru Red Hat OpenShift pomocí shellu `bash/zsh` .

   b) Nastavte následující proměnné prostředí:

```
export QM=QueueManager_name
export QM_NAMESPACE=QueueManager_namespace
export MQ_OPERATOR_NAMESPACE=mq_operator_namespace
```

Kde *QueueManager_name* je název vašeho prostředku QueueManager , *QueueManager_namespace* je obor názvů, kde je implementován, a *mq_operator_namespace* je obor názvů, kde je implementován IBM MQ Operator . Tato hodnota může být stejná jako obor názvů QueueManager .

c) Spusťte následující příkazy a poskytněte všechny výsledné výstupní soubory podpoře IBM .

```
# OCP / Kubernetes: Version
oc version -o yaml > ocversion.yaml

# QueueManager: YAML
oc get qmgr $QM -n $QM_NAMESPACE -o yaml > "queue-manager-$QM.yaml"

# MQ Queue Manager: Pods
oc get pods -n $QM_NAMESPACE -o wide --selector "app.kubernetes.io/instance=$QM" > "qm-
pods-$QM.txt"

# MQ Queue Manager: Pod YAML
oc get pods -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" > "qm-
pods-$QM.yaml"

# MQ Queue Manager: Pod Logs
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc logs -n $QM_NAMESPACE --previous "$p" > "qm-logs-
previous-$p.txt"; oc logs -n $QM_NAMESPACE $p > "qm-logs-$p.txt";done

# MQ Web UI: Console Log
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc cp -n $QM_NAMESPACE --retries=10 "$p:var/mqm/web/
installations/Installation1/servers/mqweb/logs/console.log" "web-$p-console.log"; done

# MQ Web UI: Messages Log
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc cp -n $QM_NAMESPACE --retries=10 "$p:var/mqm/web/
installations/Installation1/servers/mqweb/logs/messages.log" "web-$p-messages.log"; done

# MQ Queue Manager: routes defined by operator
oc get routes -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" > "qm-
routes-$QM.yaml"

# MQ Queue Manager: routes to QM
oc get routes -n $QM_NAMESPACE -o yaml --field-selector "spec.to.name=$QM-ibm-mq" > "qm-
routes2-$QM.yaml"

# MQ Queue Manager: stateful set
oc get statefulset -n $QM_NAMESPACE -o yaml ${QM}-ibm-mq > "qm-statefulset-$QM.yaml"

# MQ Queue Manager: services
oc get services -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" >
"qm-services-$QM.yaml"

# MQ Queue Manager: PVCs
oc get pvc -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" > "qm-
pvcs-$QM.yaml"

# MQ Operator: Version
oc get csv -n $QM_NAMESPACE | grep "^ibm-mq\|NAME" > mq-operator-csv.txt

# Cloud Pak Foundational Services: Version
oc get csv -n $QM_NAMESPACE | grep "^ibm-common-service-operator\|NAME" > common-services-
csv.txt

# Cloud Pak for Integration: Version (if applicable)
oc get csv -n $QM_NAMESPACE | grep "^ibm-integration-platform-navigator\|NAME" > cp4i-
csv.txt

# Output from runmqras (this may take a while to execute)
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do timestamp=$(TZ=UTC date +"%Y%m%d_%H%M%S");
oc exec -n $QM_NAMESPACE $p -- runmqras -workdirectory "/tmp/runmqras_$timestamp"
-section logger,mqweb,nativeha,trace; oc cp -n $QM_NAMESPACE --retries=10 "$p:tmp/
runmqras_$timestamp/" .; done

# MQ Operator: Pod Log
oc logs -n $MQ_OPERATOR_NAMESPACE $(oc get pods -n $MQ_OPERATOR_NAMESPACE --no-headers
--selector app.kubernetes.io/name=ibm-mq,app.kubernetes.io/managed-by=olm | cut -d ' ' -f
1) > mq-operator-log.txt
```

Poznámka:

Většina těchto příkazů vyžaduje přístup k oboru názvů, kde je implementován správce front. Avšak shromažďování protokolu IBM MQ Operator může navíc vyžadovat přístup **administrátora klastru** , pokud je nainstalován produkt IBM MQ Operator **s rozsahem klastru**.

Související úlohy

Shromažďování informací o odstraňování problémů pro podporu IBM

OpenShift CP4I Odstraňování problémů: Získání přístupu k datům správce front

Pomocí nástroje PVC inspector získáte přístup k souborům v PVC správce front, kde nelze vytvořit vzdálený shell pro sekci správce front. Důvodem může být skutečnost, že sekce je ve stavu **`Error`** nebo **`CrashLoopBackOff`** . Tento nástroj je navržen pro použití se správci front implementovanými produktem IBM MQ Operator.

Než začnete

Chcete-li použít nástroj PVC inspektor. musíte mít přístup k oboru názvů správce front.

Informace o této úloze

Při odstraňování problémů můžete přistupovat k datům uloženým v PVC (Persistent Volume Claims) přidružených k danému správci front. Chcete-li to provést, použijte nástroj pro připojení PVC k sadě podů inspektora. Poté můžete získat vzdálený shell do libovolného podu inspektora pro čtení souborů.

V závislosti na typu nasazení se vytvoří jedna až tři sekce inspektora. Svazky specifické pro danou sekci správce front Native-HA nebo Multi-Instance jsou k dispozici v přidružené sekci inspektoru PVC. Sdílené svazky jsou k dispozici na všech inspektorech. Název sekce inspektora obsahuje název přidružené sekce správce front.

Postup

1. Stáhněte nástroj PVC inspector produktu MQ .

   Nástroj je k dispozici zde: https://github.com/ibm-messaging/mq-pvc-tool.
2. Ujistěte se, že jste přihlášeni do svého klastru.
3. Zjistěte název správce front a obor názvů, ve kterém je spuštěn správce front.
4. Spusťte nástroj Inspektor pro vašeho správce front.
   a) Spusťte následující příkaz a zadejte název správce front a jeho obor názvů.

   ```
   ./pvc-tool.sh queue_manager_name queue_manager_namespace_name
   ```

   b) Po dokončení nástroje spusťte následující příkaz, abyste zobrazili vytvářené sekce inspektora.

   ```
   oc get pods
   ```
5. Zobrazte soubory připojené k panelu inspektora.
   a) Každá sekce inspektora PVC je přidružena k podu správce front, takže může existovat více podů inspektora. Přistupte k jedné z těchto sekcí spuštěním následujícího příkazu:

   ```
   oc rsh pvc-inspector-pod-name
   ```

   Jste umístěni do adresáře obsahujícího připojené adresáře PVC.
   b) Vypište seznam adresářů PVC spuštěním následujícího příkazu:

   ```
   ls
   ```

   c) Zobrazte seznam PVC spuštěním následujícího příkazu mimo vzdálenou relaci shellu:

```
oc get pvc
```

d) Vyčistěte sekce vytvořené nástrojem spuštěním následujícího příkazu:

```
oc delete pods -l tool=mq-pvc-inspector
```

OpenShift CP4I Odkaz rozhraní API pro IBM MQ Operator

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

OpenShift CP4I Odkaz rozhraní API pro mq.ibm.com/v1beta1

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

CP4I-LTS OpenShift CP4I CD *Odkaz na licenci pro mq.ibm.com/v1beta1*

Aktuální verze licencí

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**	**Použitelné verze IBM MQ**
`L-VTPK-22YZPK`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration 2023.4.1	9.3.4 nebo 9.3.5
`L-QYQF-8UFZBN`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration Omezené vydání 2023.4.1	9.3.4 nebo 9.3.5
`L-AMRD-XH6P3Q`	`Production`	IBM MQ Advanced a IBM MQ Advanced pro neproduktivní prostředí 9.3 -05/2023	9.3.3, 9.3.4 nebo 9.3.5
`L-AXAF-JLZ53A`	`Development`	IBM MQ Advanced for Developers (bez záruky) 9.3 -05/2023	9.3.3, 9.3.4 nebo 9.3.5
`L-YBXJ-ADJNSM`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration 2023.2.1	9.3.3
`L-PYRA-849GYQ`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration Omezené vydání 2023.2.1	9.3.3
`L-RJON-CJR2RX`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration 2022.4.1	9.3.1 nebo 9.3.2
`L-RJON-CJR2TC`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration Omezené vydání 2022.4.1	9.3.1 nebo 9.3.2
`L-UPFX-8MW49T`	`Production`	IBM MQ Advanced a IBM MQ Advanced pro neproduktivní prostředí 9.3 -02/2023	9.3.2
`L-APIG-CAUEQC`	`Development`	IBM MQ Advanced for Developers (bez záruky) 9.3	9.3.0, 9.3.1 nebo 9.3.2
`L-RJON-CD3JKX`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration 2022.2.1	9.3.0 nebo 9.3.1

Hodnota `spec.license.license`	Hodnota `spec.license.use`	Informace o licenci	Použitelné verze IBM MQ
`L-RJON-CD3JJU`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration Omezené vydání 2022.2.1	9.3.0 nebo 9.3.1
`L-APIG-CAUEBE`	`Production`	IBM MQ Advanced a IBM MQ Advanced pro neprodukční prostředí 9.3	9.3.0 nebo 9.3.1

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

Starší verze licencí

Viz Starší verze licencí v dokumentaci k produktu IBM MQ 9.2 .

OpenShift CP4I *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. IBM MQ Dokumentace: https://ibm.biz/BdPZqj. Odkaz na licenci: https://ibm.biz/BdPZfq..

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.
`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` QueueManagerSpec	Požadovaný stav správce front.
`status` QueueManagerStatus	Pozorovaný stav správce front.

.spec

Požadovaný stav správce front.

Zobrazí se v:

- “QueueManager” na stránce 180

Pole	Popis
`affinity`	Standardní pravidla afinity Kubernetes. Další informace viz https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.17/#affinity-v1-core.

Pole	Popis
annotations Anotace	Pole anotací slouží jako předávací pro anotace typu Pod. Uživatelé mohou do tohoto pole přidat libovolnou anotaci a použít ji na Pod. Zde uvedené anotace přepíší výchozí anotace, jsou-li k dispozici. Vyžaduje Operator MQ 1.3.0 nebo novější.
Pole imagePullSecrets LocalObjectReference	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.
labels Štítky	Pole štítků slouží jako předávací pro štítky typu Pod. Uživatelé mohou do tohoto pole přidat libovolný štítek a použít jej na Pod. Zde uvedené štítky přepíší výchozí štítky, jsou-li k dispozici. Vyžaduje Operator MQ 1.3.0 nebo novější.
license License	Nastavení, která řídí převzetí licence a které metriky licencí se mají používat.
pki PKI	Nastavení Public Key Infrastructure pro definování klíčů a certifikátů pro použití se zabezpečením Transport Layer Security (TLS) nebo MQ Advanced Message Security (AMS).
queueManager QueueManagerConfig	Nastavení pro kontejner správce front a základního správce front.
securityContext SecurityContext	Nastavení zabezpečení, které má být přidáno do kontextu securityContext podu správce front.
telemetry Telemetrie	Nastavení pro konfiguraci otevřené telemetrie. Vyžaduje operátor MQ 2.2.0 nebo vyšší.
template Template	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. Výchozí hodnota je 30 sekund.
tracing TracingConfig	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: řetězec 9.1.5.0-r2 by specifikoval MQ verze 9.1.5.0 s druhou revizí kontejnerového obrazu. Opravy specifické pro kontejner jsou často používány v revizích, jako např. opravy v základním obrazu.
web WebServerConfig	Nastavení pro webový server MQ.

.spec.annotations

Pole anotací slouží jako předávací pro anotace typu Pod. Uživatelé mohou do tohoto pole přidat libovolnou anotaci a použít ji na Pod. Zde uvedené anotace přepíší výchozí anotace, jsou-li k dispozici. Vyžaduje Operator MQ 1.3.0 nebo novější.

Zobrazí se v:

- ".spec" na stránce 180

.spec.imagePullSecrets

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

Zobrazí se v:

- ".spec" na stránce 180

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?.

.spec.labels

Pole štítků slouží jako předávací pro štítky typu Pod. Uživatelé mohou do tohoto pole přidat libovolný štítek a použít jej na Pod. Zde uvedené štítky přepíší výchozí štítky, jsou-li k dispozici. Vyžaduje Operator MQ 1.3.0 nebo novější.

Zobrazí se v:

- ".spec" na stránce 180

.spec.license

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

Zobrazí se v:

- ".spec" na stránce 180

Pole	Popis
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/BdPZfq .
metric string	Nastavení, které určuje, která metrika licence se má použít. Např. ProcessorValueUnit, VirtualProcessorCore nebo ManagedVirtualServer. Standardně se používá ProcessorValueUnit při použití licence MQ a VirtualProcessorCore při použití licence Cloud Pak for Integration.
use string	Nastavení, které řídí, jak se bude software používat, kde licence podporuje více použití. Platné hodnoty viz https://ibm.biz/BdPZfq .

.spec.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:

- “.spec” na stránce 180

Pole	Popis
Pole `keys` PKISource	Soukromé klíče, které mají být přidány do úložiště klíčů správce front.
Pole `trust` PKISource	Certifikáty pro přidání do úložiště klíčů správce front.

.spec.pki.keys

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

Zobrazí se v:

- “.spec.pki” na stránce 182

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

.spec.pki.keys.secret

Zadejte klíč pomocí tajného údaje Kybernetes.

Zobrazí se v:

- “.spec.pki.keys” na stránce 183

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

.spec.pki.trust

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

Zobrazí se v:

- “.spec.pki” na stránce 182

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

.spec.pki.trust.secret

Zadejte klíč pomocí tajného údaje Kybernetes.

Zobrazí se v:

- “.spec.pki.trust” na stránce 183

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

.spec.queueManager

Nastavení pro kontejner správce front a základního správce front.

Zobrazí se v:

- ".spec" na stránce 180

Pole	Popis
`availability` Availability	Nastavení dostupnosti pro správce front, například zda má být použita dvojice aktivní-pohotovostní, či nikoli nebo nativní vysoká dostupnost.
`debug` boolean	Zda protokolovat zprávy ladění z kódu specifického pro kontejner do protokolu kontejneru, či nikoli. Výchozí hodnota je false.
`image` string	Kontejnerový obraz, který bude použit.
`imagePullPolicy` string	Nastavení, které se řídí, když se kubelet pokusí stáhnout uvedený obraz. Výchozí hodnota je `IfNotPresent`.
Pole `ini` INISource	Nastavení pro dodávání souborů INI pro správce front. Vyžaduje MQ Operator 1.1.0 nebo vyšší.
`livenessProbe` QueueManagerLivenessProbe	Nastavení, která řídí sondu živosti.
`logFormat` string	Který formát protokolu má být použit pro tento kontejner. Použijte `JSON` pro protokoly formátované JSON z kontejneru. Použijte `Basic` pro textově formátované zprávy. Výchozí hodnota je `Basic`.
`metrics` QueueManagerMetrics	Nastavení pro metriky ve stylu Prometheus.
Pole `mqsc` MQSCSource	Nastavení pro dodávání MQSC pro správce front. Vyžaduje MQ Operator 1.1.0 nebo vyšší.
`name` string	Název základního správce front MQ, pokud je odlišný od metadata.name. Toto pole použijte v případě, že chcete název správce front, který neodpovídá pravidlům Kubernetes pro názvy (například název obsahující velká písmena).
`readinessProbe` QueueManagerReadinessProbe	Nastavení, které řídí sondu připravenosti.
`recoveryLogs` RecoveryLogs	Nastavení pro protokoly pro zotavení produktu MQ . Vyžaduje operátor MQ 2.4.0 nebo vyšší.
`resources` Resources	Nastavení, která řídí požadavky na prostředky.
`route` Trasa	Nastavení pro trasu správce front. Vyžaduje Operator MQ 1.4.0 nebo novější.
`startupProbe` StartupProbe	Nastavení, která řídí spouštěcí sondu. Vztahuje se pouze na implementace MultiInstance a NativeHA. Vyžaduje Operator MQ 1.5.0 nebo novější.
`storage` QueueManagerStorage	Nastavení úložiště pro řízení použití trvalých svazků a úložných tříd správce front.

.spec.queueManager.availability

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

Zobrazí se v:

- “.spec.queueManager” na stránce 184

Pole	Popis
`tls` Tls	Volitelné nastavení TLS pro konfiguraci zabezpečené komunikace mezi replikami NativeHA. Vyžaduje Operator MQ 1.5.0 nebo novější.
`type` string	Typ dostupnosti, který se má použít. Použijte `SingleInstance` pro jeden Pod, který bude automaticky restartován (v některých případech) službou Kubernetes. Parametr `MultiInstance` použijte pro dvojici podů, z nichž jeden je správce front systému `active` a druhý je v pohotovostním režimu. Použijte `NativeHA` pro replikaci nativní vysoké dostupnosti (vyžaduje MQ Operator 1.5.0 nebo vyšší). Výchozí hodnota je `SingleInstance`. Další podrobnosti viz http://ibm.biz/BdqAQa.
`updateStrategy` string	Strategie aktualizace, která má být použita pro správce front MultiInstance a NativeHA. Pomocí volby `RollingUpdate` můžete povolit automatické průběžné aktualizace, kdykoli se změní konfigurace správce front. Chcete-li zakázat automatické průběžné aktualizace, použijte volbu `OnDelete`. Změny správců front budou použity pouze v případě, že budou odstraněny pouze pody (včetně odstranění podů spouštěných externími faktory). Výchozí hodnota je `RollingUpdate`. Vyžaduje MQ Operator 1.6.0 nebo vyšší.

.spec.queueManager.availability.tls

Volitelné nastavení TLS pro konfiguraci zabezpečené komunikace mezi replikami NativeHA. Vyžaduje Operator MQ 1.5.0 nebo novější.

Zobrazí se v:

- “.spec.queueManager.availability” na stránce 185

Pole	Popis
`cipherSpec` string	Název specifikace CipherSpec pro zabezpečení NativeHA TLS.
`secretName` string	Název tajného údaje Kubernetes.

.spec.queueManager.ini

Zdroj konfiguračních souborů INI.

Zobrazí se v:

- “.spec.queueManager” na stránce 184

Pole	Popis
`configMap` ConfigMapINISource	ConfigMap reprezentuje Kubernetes ConfigMap obsahující informace INI.
`secret` SecretINISource	Secret reprezentuje tajný údaj Kubernetes obsahující informace INI.

.spec.queueManager.ini.configMap

ConfigMap reprezentuje Kubernetes ConfigMap obsahující informace INI.

Zobrazí se v:

- “.spec.queueManager.ini” na stránce 185

Pole	Popis
Pole `items`	Klíče uvnitř zdroje Kubernetes, které by měly být aplikovány.
`name` string	Název zdroje Kubernetes.

.spec.queueManager.ini.secret

Secret reprezentuje tajný údaj Kubernetes obsahující informace INI.

Zobrazí se v:

- “.spec.queueManager.ini” na stránce 185

Pole	Popis
Pole `items`	Klíče uvnitř zdroje Kubernetes, které by měly být aplikovány.
`name` string	Název zdroje Kubernetes.

.spec.queueManager.livenessProbe

Nastavení, která řídí sondu živosti.

Zobrazí se v:

- “.spec.queueManager” na stránce 184

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar. Výchozí hodnota je 1.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než je sonda zahájena. Výchozí hodnota je 90 sekund pro instanci SingleInstance. Výchozí hodnota je 0 sekund pro implementace MultiInstance a NativeHA. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu. Výchozí hodnota je 10 sekund.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch. Výchozí hodnota je 1.
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Výchozí hodnota je 5 sekund. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

.spec.queueManager.metrics

Nastavení pro metriky ve stylu Prometheus.

Zobrazí se v:

- “.spec.queueManager” na stránce 184

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

.spec.queueManager.mqsc

Zdroj konfiguračních souborů MQSC.

Zobrazí se v:

- ".spec.queueManager" na stránce 184

Pole	Popis
`configMap` ConfigMapMQSCSource	ConfigMap reprezentuje Kubernetes ConfigMap obsahující informace MQSC.
`secret` SecretMQSCSource	Secret reprezentuje tajný údaj Kubernetes obsahující informace MQSC.

.spec.queueManager.mqsc.configMap

ConfigMap reprezentuje Kubernetes ConfigMap obsahující informace MQSC.

Zobrazí se v:

- ".spec.queueManager.mqsc" na stránce 187

Pole	Popis
Pole `items`	Klíče uvnitř zdroje Kubernetes, které by měly být aplikovány.
`name` string	Název zdroje Kubernetes.

.spec.queueManager.mqsc.secret

Secret reprezentuje tajný údaj Kubernetes obsahující informace MQSC.

Zobrazí se v:

- ".spec.queueManager.mqsc" na stránce 187

Pole	Popis
Pole `items`	Klíče uvnitř zdroje Kubernetes, které by měly být aplikovány.
`name` string	Název zdroje Kubernetes.

.spec.queueManager.readinessProbe

Nastavení, které řídí sondu připravenosti.

Zobrazí se v:

- ".spec.queueManager" na stránce 184

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar. Výchozí hodnota je 1.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než je sonda zahájena. Výchozí hodnota je 10 sekund pro instanci SingleInstance. Výchozí hodnota je 0 sekund pro implementace MultiInstance a NativeHA. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu. Výchozí hodnota je 5 sekund.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch. Výchozí hodnota je 1.

Pole	Popis
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Výchozí hodnota je 3 sekundy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

.spec.queueManager.recoveryLogs

Nastavení pro protokoly pro zotavení produktu MQ . Vyžaduje operátor MQ 2.4.0 nebo vyšší.

Zobrazí se v:

- ".spec.queueManager" na stránce 184

Pole	Popis
`logFilePages` integer	Data protokolu pro zotavení jsou uložena v řadě souborů. Velikost souboru protokolu je určena v jednotkách stránek o velikosti 4 kB.

.spec.queueManager.resources

Nastavení, která řídí požadavky na prostředky.

Zobrazí se v:

- ".spec.queueManager" na stránce 184

Pole	Popis
`limits` Limits	Nastavení CPU & paměti.
`requests` Requests	Nastavení CPU & paměti.

.spec.queueManager.resources.limits

Nastavení CPU & paměti.

Zobrazí se v:

- ".spec.queueManager.resources" na stránce 188

Pole	Popis
`cpu`	
`memory`	

.spec.queueManager.resources.requests

Nastavení CPU & paměti.

Zobrazí se v:

- ".spec.queueManager.resources" na stránce 188

Pole	Popis
`cpu`	
`memory`	

.spec.queueManager.route

Nastavení pro trasu správce front. Vyžaduje Operator MQ 1.4.0 nebo novější.

Zobrazí se v:

- “.spec.queueManager” na stránce 184

Pole	Popis
`enabled` boolean	Zda povolit nebo zakázat trasu. Výchozí hodnota je true.

.spec.queueManager.startupProbe

Nastavení, která řídí spouštěcí sondu. Vztahuje se pouze na implementace MultiInstance a NativeHA. Vyžaduje Operator MQ 1.5.0 nebo novější.

Zobrazí se v:

- “.spec.queueManager” na stránce 184

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno za nezdar. Výchozí hodnota je 24.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než je sonda zahájena. Výchozí hodnota je 0 sekund. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu. Výchozí hodnota je 5 sekund.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno za úspěch. Výchozí hodnota je 1.
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Výchozí hodnota je 5 sekund. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

.spec.queueManager.storage

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

Zobrazí se v:

- “.spec.queueManager” na stránce 184

Pole	Popis
`defaultClass` string	Paměťová třída, která má být standardně použita pro všechny trvalé svazky tohoto správce front. Specifické trvalé svazky mohou definovat vlastní paměťovou třídu, která přepíše toto výchozí nastavení paměťové třídy. Je-li `type of availability` `SingleInstance` nebo `NativeHA`, může být paměťová třída typu type ReadWriteOnce nebo ReadWriteMany. Je-li `type of availability` `MultiInstance`, musí být paměťová třída typu ReadWriteMany.
`defaultDeleteClaim` boolean	Určuje, zda mají být odstraněny všechny svazky při odstranění správce front. Specifické trvalé svazky mohou definovat svou vlastní hodnotu pro deleteClaim, což přepíše toto nastavení defaultDeleteClaim. Výchozí hodnota je false.
`persistedData` QueueManagerOptionalVolume	Podrobnosti o PersistentVolume pro trvalá data pro produkt MQ, včetně konfigurace, front a zpráv. Povinné při použití správce front s více instancemi.

Pole	Popis
queueManager QueueManagerVolume	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	Podrobnosti o trvalých svazcích pro protokoly zotavení MQ. Povinné při použití správce front s více instancemi.
scratch pracovní	Nastavení pro dočasný svazek správce front. Tento svazek bude připojen jako složka '/run' na kontejneru. Použitelné pouze v případě, že je kořenový systém souborů nastaven na jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.
tmp Tmp	Nastavení pro dočasný svazek Tmp správce front. Tento svazek bude připojen ke kontejneru jako složka '/tmp'. Na tomto svazku budou vytvořeny soubory diagnostických dat, například soubor zip vytvořený příkazem runmqras. Použitelné pouze v případě, že je kořenový systém souborů nastaven na jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

.spec.queueManager.storage.persistedData

Podrobnosti o PersistentVolume pro trvalá data pro produkt MQ, včetně konfigurace, front a zpráv. Povinné při použití správce front s více instancemi.

Zobrazí se v:

- ".spec.queueManager.storage" na stránce 189

Pole	Popis
class string	Paměťová třída, která se má použít pro tento svazek. Platné pouze v případě, že type je persistent-claim. Je-li type of availability SingleInstance nebo NativeHA, může být paměťová třída typu type ReadWriteOnce nebo ReadWriteMany. Je-li type of availability MultiInstance, musí být paměťová třída typu ReadWriteMany.
deleteClaim boolean	Určuje, zda má být tento svazek odstraněn při odstranění správce front.
enabled boolean	Určuje, zda má být tento svazek povolen jako samostatný svazek, nebo umístěn ve výchozím svazku queueManager. Výchozí hodnota je false.
size string	Velikost svazku PersistentVolume, který má být předán objektu Kubernetes, včetně jednotek SI.Size of the PersistentVolume to pass to Kubernetes, including SI units Platné pouze v případě, že type je persistent-claim. Například 2Gi. Výchozí hodnota je 2Gi.
sizeLimit string	Limit velikosti při použití svazku ephemeral. Soubory jsou stále zapisovány do dočasného adresáře, takže můžete tuto volbu použít k omezení velikosti. Platné pouze v případě, že type je ephemeral a kořenový systém souborů je nastaven na jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.
type string	Typ svazku, který se má použít. Vyberte volbu ephemeral , chcete-li použít dočasné úložiště, nebo volbu persistent-claim , chcete-li použít trvalý svazek. Výchozí hodnota je persistent-claim.

.spec.queueManager.storage.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:

- “.spec.queueManager.storage” na stránce 189

Pole	Popis
`class` string	Paměťová třída, která se má použít pro tento svazek. Platné pouze v případě, že `type` je `persistent-claim`. Je-li `type of availability` `SingleInstance` nebo `NativeHA`, může být paměťová třída typu type ReadWriteOnce nebo ReadWriteMany. Je-li `type of availability` `MultiInstance`, musí být paměťová třída typu ReadWriteMany.
`deleteClaim` boolean	Určuje, zda má být tento svazek odstraněn při odstranění správce front.
`size` string	Velikost svazku PersistentVolume, který má být předán objektu Kubernetes, včetně jednotek SI.Size of the PersistentVolume to pass to Kubernetes, including SI units Platné pouze v případě, že `type` je `persistent-claim`. Například `2Gi`. Výchozí hodnota je `2Gi`.
`sizeLimit` string	Limit velikosti při použití svazku `ephemeral`. Soubory jsou stále zapisovány do dočasného adresáře, takže můžete tuto volbu použít k omezení velikosti. Platné pouze v případě, že `type` je `ephemeral` a kořenový systém souborů je nastaven na jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.
`type` string	Typ svazku, který se má použít. Vyberte volbu `ephemeral` , chcete-li použít dočasné úložiště, nebo volbu `persistent-claim` , chcete-li použít trvalý svazek. Výchozí hodnota je `persistent-claim`.

.spec.queueManager.storage.recoveryLogs

Podrobnosti o trvalých svazcích pro protokoly zotavení MQ. Povinné při použití správce front s více instancemi.

Zobrazí se v:

- “.spec.queueManager.storage” na stránce 189

Pole	Popis
`class` string	Paměťová třída, která se má použít pro tento svazek. Platné pouze v případě, že `type` je `persistent-claim`. Je-li `type of availability` `SingleInstance` nebo `NativeHA`, může být paměťová třída typu type ReadWriteOnce nebo ReadWriteMany. Je-li `type of availability` `MultiInstance`, musí být paměťová třída typu ReadWriteMany.
`deleteClaim` boolean	Určuje, zda má být tento svazek odstraněn při odstranění správce front.
`enabled` boolean	Určuje, zda má být tento svazek povolen jako samostatný svazek, nebo umístěn ve výchozím svazku `queueManager`. Výchozí hodnota je false.
`size` string	Velikost svazku PersistentVolume, který má být předán objektu Kubernetes, včetně jednotek SI.Size of the PersistentVolume to pass to Kubernetes, including SI units Platné pouze v případě, že `type` je `persistent-claim`. Například `2Gi`. Výchozí hodnota je `2Gi`.
`sizeLimit` string	Limit velikosti při použití svazku `ephemeral`. Soubory jsou stále zapisovány do dočasného adresáře, takže můžete tuto volbu použít k omezení velikosti. Platné pouze v případě, že `type` je `ephemeral` a kořenový systém souborů je nastaven na jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.
`type` string	Typ svazku, který se má použít. Vyberte volbu `ephemeral` , chcete-li použít dočasné úložiště, nebo volbu `persistent-claim` , chcete-li použít trvalý svazek. Výchozí hodnota je `persistent-claim`.

.spec.queueManager.storage.scratch

Nastavení pro dočasný svazek správce front. Tento svazek bude připojen jako složka '/run' na kontejneru. Použitelné pouze v případě, že je kořenový systém souborů nastaven na jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

Zobrazí se v:

- ".spec.queueManager.storage" na stránce 189

Pole	Popis
`sizeLimit` string	Omezení velikosti přechodného objemu, včetně jednotek SI. Například `2Gi`. Platí pouze v případě, že je kořenový systém souborů nastaven na hodnotu jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

.spec.queueManager.storage.tmp

Nastavení pro dočasný svazek Tmp správce front. Tento svazek bude připojen ke kontejneru jako složka '/tmp'. Na tomto svazku budou vytvořeny soubory diagnostických dat, například soubor zip vytvořený příkazem runmqras. Použitelné pouze v případě, že je kořenový systém souborů nastaven na jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

Zobrazí se v:

- ".spec.queueManager.storage" na stránce 189

Pole	Popis
`sizeLimit` string	Omezení velikosti přechodného objemu, včetně jednotek SI. Například `2Gi`. Platí pouze v případě, že je kořenový systém souborů nastaven na hodnotu jen pro čtení. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

.spec.securityContext

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

Zobrazí se v:

- ".spec" na stránce 180

Pole	Popis
`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`, jestliže používáte poskytovatele úložiště, který vyžaduje, abyste byli kořenovým uživatelem pro přístup k nově zajišťovaným svazkům. Nastavení této hodnoty na `true` ovlivňuje, který objekt SCC (Security Context Constraints) můžete použít, a správce front se nemusí spustit, pokud nemáte autorizaci k použití objektu SCC, který umožňuje kořenovému uživateli. Výchozí hodnota je false. Další informace viz https://docs.openshift.com/container-platform/latest/authentication/managing-security-context-constraints.html.
`readOnlyRootFilesystem` boolean	Zda povolit nebo nepovolit nastavení kořenového systému souborů jen pro čtení pro správce front. Výchozí hodnota je false. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

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.

.spec.telemetry

Nastavení pro konfiguraci otevřené telemetrie. Vyžaduje operátor MQ 2.2.0 nebo vyšší.

Zobrazí se v:

- ".spec" na stránce 180

Pole	Popis
`tracing` Trasování	Nastavení pro trasování otevřené telemetrie.

.spec.telemetry.tracing

Nastavení pro trasování otevřené telemetrie.

Zobrazí se v:

- ".spec.telemetry" na stránce 193

Pole	Popis
`instana` Instana	Nastavení pro trasování instance.

.spec.telemetry.tracing.instana

Nastavení pro trasování instance.

Zobrazí se v:

- ".spec.telemetry.tracing" na stránce 193

Pole	Popis
`agentHost` string	Název hostitele agenta Instana, na který se mají odeslat data trasování. Tato volba by neměla obsahovat protokol.
`enabled` boolean	Zda povolit nebo nepovolit trasování instance. Výchozí hodnota je false.
`protocol` string	Protokol, který se má použít při komunikaci s agentem Instana. http a https jsou podporovány.

.spec.template

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:

- ".spec" na stránce 180

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

.spec.tracing

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

Zobrazí se v:

- ".spec" na stránce 180

Pole	Popis
`agent` TracingAgent	Pouze v produktu Cloud Pak for Integration můžete konfigurovat nastavení pro volitelného agenta trasování.
`collector` TracingCollector	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. Výchozí hodnota je false.
`namespace` string	Obor názvů, kde je nainstalován produkt Cloud Pak for Integration Operations Dashboard.

.spec.tracing.agent

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

Zobrazí se v:

- ".spec.tracing" na stránce 194

Pole	Popis
`image` string	Kontejnerový obraz, který bude použit.
`imagePullPolicy` string	Nastavení, které se řídí, když se kubelet pokusí stáhnout uvedený obraz. Výchozí hodnota je `IfNotPresent`.
`livenessProbe` TracingProbe	Nastavení, která řídí sondu živosti.
`readinessProbe` TracingProbe	Nastavení, které řídí sondu připravenosti.

.spec.tracing.agent.livenessProbe

Nastavení, která řídí sondu živosti.

Zobrazí se v:

- ".spec.tracing.agent" na stránce 194

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar. Výchozí hodnota je 1.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než budou zahájeny sondy živosti. Výchozí hodnota je 10 sekund. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu. Výchozí hodnota je 10 sekund.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch. Výchozí hodnota je 1.

Pole	Popis
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Výchozí hodnota je 2 sekundy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

.spec.tracing.agent.readinessProbe

Nastavení, které řídí sondu připravenosti.

Zobrazí se v:

- ".spec.tracing.agent" na stránce 194

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar. Výchozí hodnota je 1.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než budou zahájeny sondy živosti. Výchozí hodnota je 10 sekund. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu. Výchozí hodnota je 10 sekund.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch. Výchozí hodnota je 1.
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Výchozí hodnota je 2 sekundy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

.spec.tracing.collector

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

Zobrazí se v:

- ".spec.tracing" na stránce 194

Pole	Popis
`image` string	Kontejnerový obraz, který bude použit.
`imagePullPolicy` string	Nastavení, které se řídí, když se kubelet pokusí stáhnout uvedený obraz. Výchozí hodnota je `IfNotPresent`.
`livenessProbe` TracingProbe	Nastavení, která řídí sondu živosti.
`readinessProbe` TracingProbe	Nastavení, které řídí sondu připravenosti.

.spec.tracing.collector.livenessProbe

Nastavení, která řídí sondu živosti.

Zobrazí se v:

- ".spec.tracing.collector" na stránce 195

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar. Výchozí hodnota je 1.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než budou zahájeny sondy živosti. Výchozí hodnota je 10 sekund. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu. Výchozí hodnota je 10 sekund.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch. Výchozí hodnota je 1.
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Výchozí hodnota je 2 sekundy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

.spec.tracing.collector.readinessProbe

Nastavení, které řídí sondu připravenosti.

Zobrazí se v:

- ".spec.tracing.collector" na stránce 195

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar. Výchozí hodnota je 1.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než budou zahájeny sondy živosti. Výchozí hodnota je 10 sekund. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu. Výchozí hodnota je 10 sekund.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch. Výchozí hodnota je 1.
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Výchozí hodnota je 2 sekundy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

.spec.web

Nastavení pro webový server MQ.

Zobrazí se v:

- ".spec" na stránce 180

Pole	Popis
`console` Konzola	Nastavení pro webovou konzolu produktu MQ . Vyžaduje operátor MQ 3.0.0 nebo vyšší.
`enabled` boolean	Zda povolit nebo zakázat webový server. Výchozí hodnota je false.
`manualConfig` ManualConfig	Nastavení pro dodání konfigurace XML webového serveru. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

.spec.web.console

Nastavení pro webovou konzolu produktu MQ . Vyžaduje operátor MQ 3.0.0 nebo vyšší.

Zobrazí se v:

- ".spec.web" na stránce 196

Pole	Popis
`authentication` Ověření	Nastavení ověřování pro webovou konzolu produktu MQ . Vyžaduje operátor MQ 3.0.0 nebo vyšší.
`authorization` Autorizace	Nastavení autorizace pro webovou konzolu produktu MQ . Vyžaduje operátor MQ 3.0.0 nebo vyšší.

.spec.web.console.authentication

Nastavení ověřování pro webovou konzolu produktu MQ . Vyžaduje operátor MQ 3.0.0 nebo vyšší.

Zobrazí se v:

- ".spec.web.console" na stránce 197

Pole	Popis
`provider` string	Poskytovatel ověřování, který má být použit pro webovou konzolu produktu MQ . Použijte `integration-keycloak` , chcete-li použít jednotné přihlášení s uživatelským rozhraním platformy Cloud Pak for Integration (Keycloak). Výchozí nastavení je `integration-keycloak` , pokud používáte licenci na produkt Cloud Pak for Integration , nebo `manual` pokud používáte licenci na produkt MQ . Použijte `manual` , chcete-li poskytnout svou vlastní konfiguraci.

.spec.web.console.authorization

Nastavení autorizace pro webovou konzolu produktu MQ . Vyžaduje operátor MQ 3.0.0 nebo vyšší.

Zobrazí se v:

- ".spec.web.console" na stránce 197

Pole	Popis
`provider` string	Poskytovatel autorizace, který má být použit pro webovou konzolu produktu MQ . Použijte `integration-keycloak` , chcete-li použít role poskytnuté produktem Cloud Pak for Integration Keycloak. Použijte `manual` , chcete-li poskytnout svou vlastní konfiguraci. Výchozí nastavení je `integration-keycloak` , pokud používáte licenci na produkt Cloud Pak for Integration , nebo `manual` pokud používáte licenci na produkt MQ .

.spec.web.manualConfig

Nastavení pro dodání konfigurace XML webového serveru. Vyžaduje operátor MQ 3.0.0 nebo vyšší.

Zobrazí se v:

- ".spec.web" na stránce 196

Pole	Popis
`configMap` ConfigMap	ConfigMap představuje Kubernetes ConfigMap , která obsahuje konfiguraci XML webového serveru.

Pole	Popis
`secret` Secret	Tajný klíč představuje tajný klíč Kubernetes , který obsahuje konfiguraci XML webového serveru. Použití tajného klíče chrání všechna pověření ve vrstvě Kubernetes , ale je možné, že nástroje pro monitorování a odstraňování problémů mohou vystavit základní soubor nezabezpečeně. Chcete-li zlepšit zabezpečení, zakódujte pověření pomocí "securityUtility".

.spec.web.manualConfig.configMap

ConfigMap představuje Kubernetes ConfigMap , která obsahuje konfiguraci XML webového serveru.

Zobrazí se v:

- “.spec.web.manualConfig” na stránce 197

Pole	Popis
`name` string	Název zdroje Kubernetes.

.spec.web.manualConfig.secret

Tajný klíč představuje tajný klíč Kubernetes , který obsahuje konfiguraci XML webového serveru. Použití tajného klíče chrání všechna pověření ve vrstvě Kubernetes , ale je možné, že nástroje pro monitorování a odstraňování problémů mohou vystavit základní soubor nezabezpečeně. Chcete-li zlepšit zabezpečení, zakódujte pověření pomocí "securityUtility".

Zobrazí se v:

- “.spec.web.manualConfig” na stránce 197

Pole	Popis
`name` string	Název zdroje Kubernetes.

.status

Pozorovaný stav správce front.

Zobrazí se v:

- “QueueManager” na stránce 180

Pole	Popis
`adminUiUrl` string	Adresa URL pro uživatelské rozhraní administrace.
`availability` Availability	Stav dostupnosti správce front.
Pole `conditions` QueueManagerStatusCondition	Podmínky reprezentují nejnovější dostupná pozorování stavu správce front.
Pole `endpoints` QueueManagerStatusEndpoint	Informace v koncových bodech, které tento správce front vystavuje, jako např. koncové body rozhraní API nebo uživatelské rozhraní.
`metadata` Metadata	Metadata představují další informace pro správce front, včetně stavu integrace-Keycloak .
`name` string	Název správce front.
`phase` string	Fáze stavu správce front.

Pole	Popis
versions QueueManagerStatusVersion	Verze používaného produktu MQ a další verze dostupné z produktu IBM Entitled Registry.

.status.availability

Stav dostupnosti správce front.

Zobrazí se v:

- “.status” na stránce 198

Pole	Popis
initialQuorumEstablished boolean	Určuje, zda bylo počáteční kvorum ustanoveno pro NativeHA.

.status.conditions

QueueManagerStatusCondition definuje podmínky správce front.

Zobrazí se v:

- “.status” na stránce 198

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

.status.endpoints

QueueManagerStatusEndpoint definuje koncové body správce front.

Zobrazí se v:

- “.status” na stránce 198

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.

.status.metadata

Metadata představují další informace pro správce front, včetně stavu integrace-Keycloak .

Zobrazí se v:

- “.status” na stránce 198

Pole	Popis
`integrationKeycloak` IntegrationKeycloak	QueueManagerStatusIntegrationKeycloak definuje stav integrace-Keycloak pro QueueManager.

.status.metadata.integrationKeycloak

QueueManagerStatusIntegrationKeycloak definuje stav integrace-Keycloak pro QueueManager.

Zobrazí se v:

- ".status.metadata" na stránce 199

Pole	Popis
`clientName` string	

.status.versions

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

Zobrazí se v:

- ".status" na stránce 198

Pole	Popis
`available` QueueManagerStatusVersionAvailable	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.

.status.versions.available

Další verze produktu MQ dostupné z produktu IBM Entitled Registry.

Zobrazí se v:

- ".status.versions" na stránce 200

Pole	Popis
Pole `channels`	Kanály, které jsou k dispozici pro automatickou aktualizaci verze MQ.
Pole `versions` Versions	Specifické verze produktu MQ, které jsou k dispozici.

.status.versions.available.versions

QueueManagerStatusVersion definuje verzi produktu MQ.

Zobrazí se v:

- ".status.versions.available" na stránce 200

Pole	Popis
Pole `licenses` Licence	Licence, které jsou použitelné pro tuto verzi správce front QueueManager.
`name` string	Verze `name` pro tuto verzi QueueManager. Toto jsou platné hodnoty pro pole `spec.version`.

.status.versions.available.versions.licenses

QueueManagerStatusLicense definuje licenci.

Zobrazí se v:

- ".status.versions.available.versions" na stránce 200

Pole	Popis
`displayName` string	Zobrazovaný název pro licenci.
`link` string	Odkaz na obsah licence.
`matchesCurrentType` boolean	Zda se licence shoduje s typem momentálně používané licence.
`name` string	Název licence.

Stavové podmínky pro správce front (mq.ibm.com/v1beta1)

Pole **`status.conditions`** se aktualizují tak, aby odrážely podmínku prostředku `QueueManager`. Obecně podmínky popisují nestandardní situace. Správce front ve zdravém, připraveném stavu nemá žádné podmínky **`Error`** (chyba) nebo **`Pending`** (nevyřízené). Může mít nějaké doporučovací podmínky typu **`Warning`** (varování).

Podpora podmínek byla zavedena v produktu IBM MQ Operator 1.2.

Pro prostředek `QueueManager` jsou definovány tyto podmínky:

Tabulka 1. Stavové podmínky správce front			
Komponenta	**Typ podmínky**	**Kód příčiny**	**Varovná zpráva**
QueueManager[9]	Blokované	OperatorDependency	Pro instalaci tato instance vyžaduje, aby byl Keycloak nakonfigurován produktem [IBM Cloud Pak for Integration]. Tato instance zůstane ve stavu [Nevyřízeno], dokud nebude Keycloak ohlášen jako [KeycloakReady] v prostředku Cp4iServicesBinding pro tento QueueManager.
			Chcete-li provést instalaci, tato instance vyžaduje operátor [IBM IAM]. Tato instance zůstane ve stavu [Blokováno], dokud nebude operátor nainstalován [IBM Cloud Pak Foundational services].
	Nevyřízeno	Creating	Probíhá implementace správce front MQ
	Nevyřízeno	OidcPending	Správce front MQ čeká na registraci klienta OIDC
	Chyba	Nezdar	Implementace správce front MQ se nezdařila
	Varování	UnsupportedVersion	[10]Operand byl instalován operátorem, který není verzí *<ocp_version>* podporován. Tento operand není podporován.
	Varování	Podpora CP4I-LTS	[11]Operand CP4I-LTS *< mq_version>* byl nainstalován, ale je spravován operátorem, který se nekvalifikuje pro prodlouženou dobu trvání podpory. Tento operand nelze kvalifikovat pro dobu rozšířené podpory.
	Varování	Podpora CP4I-LTS	[12]Operand CP4I-LTS *< mq_version>* byl nainstalován, ale OCP verze 4*< ocp_version>* se nekvalifikuje pro prodlouženou dobu trvání podpory. Tento operand nelze kvalifikovat pro dobu rozšířené podpory.
	Varování	Podpora CP4I-LTS	[13]Operand CP4I-LTS *< mq_version>* byl nainstalován, ale verze OCP *< ocp_version>* se nekvalifikuje pro prodlouženou dobu trvání podpory. Tento operand je podporován podle pravidelného vydání CD.

[9] Podmínky `Creating` a `Failed` monitorují celkový průběh implementace správce front. Pokud používáte licenci na produkt IBM Cloud Pak for Integration a webová konzola je povolena, podmínka `OidcPending` zaprotokoluje stav správce front při čekání na dokončení registrace klienta OIDC pomocí IAM.

[10] Operator 1.4.0 a novější

Tabulka 1. Stavové podmínky správce front (pokračování)			
Komponenta	**Typ podmínky**	**Kód příčiny**	**Varovná zpráva**
Pod[14]	Nevyřízeno	PodPending	Probíhá implementace Pod pro správce front MQ
	Chyba	PodFailed	Probíhá implementace Pod pro správce front MQ
Úložný prostor[15]	Nevyřízeno	StoragePending	Probíhá zajišťování úložiště pro správce front MQ
	Varování	StorageEphemeral	Použití dočasného úložiště pro produkčního správce front MQ
	Chyba	StorageFailed	Úložiště pro správce front MQ se nezdařilo zajistit

Multi Sestavení vlastního kontejneru IBM MQ a kódu implementace

Vyviňte svůj vlastní kontejner. Jedná se o nejflexibilnější řešení kontejneru, které ale od vás vyžaduje značné dovednosti v konfiguraci kontejnerů a abyste "vlastnili" výsledný kontejner.

Než začnete

Před vývojem vlastního kontejneru zvažte, zda můžete místo toho použít IBM MQ Operator. Viz “Zvolení, jak se má produkt IBM MQ používat v kontejnerech” na stránce 5

Informace o této úloze

Procedura

- “Plánování vlastního obrazu správce front IBM MQ pomocí kontejneru” na stránce 203
- “Sestavení ukázkového kontejnerového obrazu správce front produktu IBM MQ” na stránce 204
- “Spuštění lokálních aplikací vazby v samostatných kontejnerech” na stránce 207
- Přezkoumejte IBM MQ ukázkový graf Helm.

Multi 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.

---

11 Operator 1.4.0 a novější
12 Operator 1.4.0 a novější
13 Pouze Operator 1.3.0
14 Podmínky Pod monitorují stav podů během implementace správce front. Když se zobrazí podmínka `PodFailed`, pak bude celková podmínka správce front rovněž nastavena na `Failed`.
15 Podmínky úložiště monitorují průběh (podmínka `StoragePending`) požadavků na vytvoření svazků pro trvalé úložiště a hlásí zpět chyby vazby a další selhání. Jestliže dojde k jakékoli chybě během zajišťování úložiště, bude podmínka `StorageFailed` přidána do seznamu podmínek a celková podmínka správce front bude rovněž nastavena na `Failed`.

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.

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

Zabezpečení kontejneru

Aby byly minimalizovány nároky na zabezpečení běhového prostředí, jsou ukázkové kontejnerové obrazy nainstalovány s použitím rozbalitelné instalace produktu IBM MQ. Tím je zajištěno, že nejsou nastaveny žádné bity `setuid` a že kontejner nemusí ani používat eskalaci oprávnění. Některé systémy kontejnerů definují, která ID uživatelů se mohou používat. Rozbalitelná instalace nečiní žádné předpoklady o dostupných uživatelích operačního systému.

Multi Sestavení ukázkového kontejnerového obrazu správce front produktu IBM MQ

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 204
  - “Sestavení ukázkového obrazu nakonfigurovaného správce front IBM MQ” na stránce 205

Multi 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.
- Volitelné: Pokud plánujete konfigurovat zabezpečený přístup pomocí Red Hat OpenShift Container Platform "omezeného" omezení SCC (Security Context Constraint), použijte jeden z neinstalačních obrazů IBM MQ .

  Odkazy na stažení těchto obrazů jsou k dispozici v části Kontejnery v části IBM MQ Soubory ke stažení.

Výsledky

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

Nyní jste připraveni sestavit ukázkový nakonfigurovaný obraz správce front IBM MQ.

Multi 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

Tato úloha předpokládá, že při sestavení ukázkového základního obrazu správce front IBM MQ jste použili balík "No-Install" IBM MQ. Jinak nemůžete konfigurovat zabezpečený přístup pomocí Red Hat OpenShift Container Platform "omezeného" objektu Security Context Constraint (SCC). "Omezený" objekt SCC, který se používá ve výchozím nastavení, používá náhodná ID uživatelů a zabraňuje eskalaci oprávnění změnou na jiného uživatele. Tradiční instalační program produktu IBM MQ založený na balících RPM se spoléhá na uživatele a skupinu `mqm` a také používá bity `setuid` na spustitelných programech. Když v aktuální verzi produktu IBM MQpoužijete balík "No-Install" IBM MQ , neexistuje již žádný uživatel `mqm` , ani skupina `mqm` .

Postup

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

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

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

3. Sestavte vlastní kontejnerový obraz pomocí následujícího příkazu:

```
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.

   Poznámka: V systému Red Hat Enterprise Linux (RHEL) můžete použít příkaz **`docker`** (RHEL V7) nebo **podman** (RHEL V7 nebo RHEL V8). V systému Linux bude nutné spustit příkazy **`docker`** pomocí příkazu **sudo** na začátku příkazu, abyste získali dodatečná oprávnění.
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:

```
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

Sestavili jste nakonfigurovaný kontejnerový obraz a můžete jej zobrazit pomocí příkazu **`docker ps`**. Procesy produktu IBM MQ spuštěné ve vašem kontejneru si můžete zobrazit pomocí příkazu **`docker top`**.

Upozornění:

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

Jak pokračovat dále

- Pokud se kontejner nezobrazí, když použijete příkaz **`docker ps`**, mohlo dojít k nezdaru kontejneru. Kontejnery, které se nezdařily, můžete zobrazit pomocí příkazu **`docker ps -a`** .
- Použijete-li příkaz **`docker ps -a`**, zobrazí se ID kontejneru. Toto ID bylo také vytištěno, jste zadali příkaz **`docker run`**.
- Protokoly kontejneru si můžete zobrazit pomocí příkazu **`docker logs ${CONTAINER_ID}`**.

Multi Spuštění lokálních aplikací vazby v samostatných kontejnerech

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

Informace o této úloze

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`

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 208.

Multi 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 207.

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
```

MQ Adv. Vytvoření nativní skupiny HA, pokud vytváříte vlastní kontejnery

Chcete-li vytvořit skupinu Nativní HA, musíte vytvořit, nakonfigurovat a spustit tři správce front.

Informace o této úloze

Doporučenou metodou pro vytvoření řešení nativní HA je použití operátoru IBM MQ (viz Nativní HA). Případně, pokud vytvoříte vlastní kontejnery, můžete postupovat podle těchto pokynů.

Chcete-li vytvořit skupinu Nativní HA, vytvořte tři správce front na třech uzlech s typem protokolu nastaveným na `log replication`. Poté upravíte soubor `qm.ini` pro každého správce front a přidáte podrobnosti o připojení pro každý ze tří uzlů tak, aby mohly vzájemně replikovat data protokolu.

Poté musíte spustit všechny tři správce front, aby mohli zkontrolovat, zda všechny tři instance mohou vzájemně komunikovat, a určit, která z nich bude aktivní instancí a která bude replikou.

Poznámka: Tímto způsobem můžete vytvořit nativní skupinu HA ve svých vlastních kontejnerech, pouze pokud spouštíte Kubernetes nebo Red Hat OpenShift.

Postup

1. V každém ze tří uzlů vytvořte správce front s určením typu protokolu repliky protokolu a zadáním jedinečného názvu pro každou instanci protokolu. Každý správce front má stejný název:

   ```
   crtmqm -lr instance_name qmname
   ```

   Příklad:

   ```
   node 1> crtmqm -lr qm1_inst1 qm1

   node 2> crtmqm -lr qm1_inst2 qm1

   node 3> crtmqm -lr qm1_inst3 qm1
   ```

2. Při úspěšném vytvoření každého správce front je do konfiguračního souboru správce front `qm.ini`přidána další sekce s názvem `NativeHALocalInstance` . Do sekce se přidá atribut `Name` , který uvádí zadaný název instance.

   Volitelně můžete přidat následující atributy do sekce `NativeHALocalInstance` v souboru `qm.ini` :

   `KeyRepository`
   Umístění úložiště klíčů, které obsahuje digitální certifikát, který se má použít pro ochranu provozu replikace protokolu. Umístění je uvedeno v kmenovém formátu, to znamená, že obsahuje úplnou cestu a název souboru bez přípony. Je-li atribut stanza `KeyRepository` vynechán, data replikace protokolu se vyměňují mezi instancemi v prostém textu.

   `CertificateLabel`
   Popisek certifikátu identifikující digitální certifikát, který se má použít pro ochranu provozu replikace protokolu. Pokud je zadán parametr `KeyRepository` , ale parametr `CertificateLabel` je vynechán, použije se výchozí hodnota `ibmwebspheremq`*`queue_manager`* .

   `CipherSpec`
   MQ CipherSpec , která má být použita k ochraně provozu replikace protokolu. Je-li uveden tento atribut stanza, musí být také uveden parametr `KeyRepository` . Pokud je zadán parametr `KeyRepository` , ale parametr `CipherSpec` je vynechán, použije se výchozí hodnota `ANY` .

LocalAddress
Adresa lokálního síťového rozhraní, která přijímá provoz replikace protokolu. Je-li uveden tento atribut stanza, identifikuje lokální síťové rozhraní a/nebo port ve formátu "[addr] [(port)]". Síťovou adresu lze zadat jako název hostitele, IPv4 tečkový desítkový formát nebo IPv6 hexadecimální formát. Pokud je tento atribut vynechán, správce front se pokusí svázat se všemi síťovými rozhraními, použije port uvedený v `ReplicationAddress` v sekci `NativeHAInstances` odpovídající názvu lokální instance.

HeartbeatInterval
Interval prezenčního signálu definuje, jak často, v milisekundách, aktivní instance správce front nativní vysoké dostupnosti odešle synchronizaci sítě. Platný rozsah hodnoty intervalu prezenčního signálu je 500 (0,5 s) do 60000 (1 min), hodnota mimo tento rozsah způsobí, že se správce front nespustí. Je-li tento atribut vynechán, použije se výchozí hodnota 5000 (5 s). Každá instance musí používat stejný interval prezenčního signálu.

HeartbeatTimeout
Časový limit prezenčního signálu definuje, jak dlouho bude instance repliky správce front nativní vysoké dostupnosti čekat, než se rozhodne, že aktivní instance nereaguje. Platný rozsah hodnoty časového limitu intervalu prezenčního signálu je 500 (0,5 s) do 120000 (2 min). Hodnota časového limitu prezenčního signálu musí být větší než nebo rovna intervalu prezenčního signálu.

Neplatná hodnota způsobí, že se správce front nespustí. Je-li tento atribut vynechán, čeká replika 2 x `HeartbeatInterval` před spuštěním procesu pro výběr nové aktivní instance. Každá instance musí používat stejný časový limit prezenčního signálu.

RetryInterval
Interval opakování definuje, jak často by se měl správce front nativní vysoké dostupnosti, v milisekundách, opakovat nezdařený odkaz na replikaci. Platný rozsah intervalu opakování je 500 (0,5 s) do 120000 (2 min). Je-li tento atribut vynechán, čeká replika 2 x `HeartbeatInterval` před zopakováním nezdařeného odkazu na replikaci.

3. Upravte soubor `qm.ini` pro každého správce front a přidejte podrobnosti připojení. Přidáte tři sekce `NativeHAInstance` , jednu pro každou instanci správce front v nativní skupině HA (včetně lokální instance). Přidejte následující atributy:

   Název
   Zadejte název instance, který jste použili při vytváření instance správce front.

   ReplicationAddress
   Uveďte název hostitele, adresu instance v hexadecimálním formátu IPv4 s tečkami nebo adresu instance v hexadecimálním formátu IPv6 . Adresu můžete uvést jako název hostitele, IPv4 tečkovou desítkovou adresu nebo IPv6 adresu v hexadecimálním formátu. Replikační adresa musí být rozpoznatelná a směrovatelná z každé instance ve skupině. Číslo portu, které se má použít pro replikaci protokolu, musí být uvedeno v závorkách, například:

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

   Poznámka: Sekce `NativeHAInstance` jsou identické na každé instanci a lze je poskytnout pomocí automatické konfigurace (**crtmqm -ii**).

4. Spusťte každou ze tří instancí:

   ```
   strmqm QMgrName
   ```

   Když jsou instance spuštěny, komunikují a kontrolují, zda jsou všechny tři instance spuštěny, a poté rozhodují, která z těchto tří instancí je aktivní, zatímco ostatní dvě instance pokračují ve spouštění jako repliky.

Příklad

Následující příklad zobrazuje sekci souboru `qm.ini` uvádějící požadované podrobnosti nativní vysoké dostupnosti pro jednu ze tří instancí:

```
NativeHALocalInstance:
  LocalName=node-1

NativeHAInstance:
  Name=node-1
  ReplicationAddress=host1.example.com(4444)
NativeHAInstance:
  Name=node-2
  ReplicationAddress=host2.example.com(4444)
NativeHAInstance:
  Name=node-3
  ReplicationAddress=host3.example.com(4444)
```

MQ Adv. Faktory ovlivňující provádění vlastní průběžné aktualizace správce front nativní vysoké dostupnosti

Jakákoli aktualizace verze produktu IBM MQ nebo specifikace podu pro správce front nativní vysoké dostupnosti bude vyžadovat provedení průběžné aktualizace instancí správce front. Produkt IBM MQ Operator ji automaticky zpracuje, ale pokud sestavujete vlastní kód implementace, pak jsou zde některé důležité aspekty.

Poznámka: Ukázka Helmova grafu obsahuje skript shellu k provedení průběžné aktualizace, ale tento skript **není** vhodný pro provozní použití, protože se nezabývá otázkami v tomto tématu.

Kubernetes V produktu Kubernetes se prostředky `StatefulSet` používají ke správě seřazených aktualizací při spuštění a průběžných aktualizací. Součástí procedury spuštění je spuštění každého podu jednotlivě, vyčkání na jeho připravenost a pak přesun na další pod. To nebude fungovat pro nativní HA, protože všechny pody musí být spuštěny, aby mohly spustit volby vůdce. Proto musí být pole `.spec.podManagementPolicy` v produktu `StatefulSet` nastaveno na `Parallel`. To také znamená, že budou všechny pody aktualizovány také paralelně, což je zvláště nežádoucí. Z tohoto důvodu by měl produkt `StatefulSet` také použít strategii aktualizace `OnDelete`.

Neschopnost používat kód průběžné aktualizace `StatefulSet` vyžaduje potřebu vlastního kódu průběžné aktualizace, který by měl zvážit následující:

- Postup běžné průběžné aktualizace
- Minimalizace výpadku aktualizací podů v nejlepším pořadí
- Zpracování změn ve stavu klastru
- Ošetření chyb
- Práce s problémy časování

Postup běžné průběžné aktualizace

Kód průběžné aktualizace by měl čekat na každou instanci, aby se zobrazil stav `REPLICA` z `dspmq`. To znamená, že instance provedla určitou úroveň spuštění (je například spuštěn kontejner a jsou spuštěny procesy MQ), ale zatím nutně nemusela vést konverzaci s ostatními instancemi. Například: Pod A se restartuje a jakmile je ve stavu `REPLICA` , pod B se restartuje. Jakmile je spuštěn Pod B s novou konfigurací, měl by být schopen komunikovat s Podem A a může formovat kvorum, a buď A, nebo B se stane novou aktivní instancí.

Je proto užitečné mít zpoždění poté, co každý pod dosáhne stavu `REPLICA`, aby mu bylo umožněno připojit se ke svým protějškům a ustavit kvorum.

Minimalizace výpadku aktualizací podů v nejlepším pořadí

Kód průběžné aktualizace by měl odstranit pody jeden po druhém, počínaje pody, které jsou ve známém chybovém stavu, a poté jakékoli pody, které se nespustily úspěšně. Aktivní pod správce front by měl být obecně aktualizován naposledy.

Je také důležité pozastavit odstranění podů, pokud poslední aktualizace vedla k tomu, že pod vstoupil do známého chybového stavu. Tím se zabrání provedení přerušené aktualizace ve všech podech. K tomu může dojít například v případě, když je pod aktualizován pro použití nového obrazu kontejneru, který není přístupný (nebo obsahuje překlep).

Zpracování změn ve stavu klastru

Kód průběžné aktualizace musí vhodně reagovat na změny v reálném čase ve stavu klastru. Jeden z podů správce front může být například vypovězen kvůli opětnému zavedení uzlu nebo kvůli tlaku uzlu. Je možné, že nemusí být vypovězený pod ihned znovu naplánován, pokud je klastr zaneprázdněn. V takovém případě by měl být kód průběžné aktualizace před restartováním jakýchkoli jiných podů čekat odpovídajícím způsobem.

Ošetření chyb

Kód průběžní aktualizace musí být odolný vůči selháním při volání rozhraní API Kubernetes a jiného neočekávaného chování klastru.

Kromě toho musí být samotný kód průběžné aktualizace tolerantní k restartování. Průběžná aktualizace může být spuštěna dlouho a může být nutné restartovat kód.

Práce s problémy časování

Kód průběžné aktualizace potřebuje zkontrolovat revize aktualizace podu, aby mohl zajistit, že je pod restartován. Tím se vyvarujete problémů s časováním, kdy může pod označovat, že je "Spuštěný", ale ve skutečnosti ještě není ukončený.

Související pojmy

“Zvolení, jak se má produkt IBM MQ používat v kontejnerech” na stránce 5
Existuje více voleb pro použití produktu IBM MQ v kontejnerech: můžete zvolit použití IBM MQ Operator, který používá předem seskupené kontejnerové obrazy nebo můžete sestavit vlastní obrazy a kód implementace.

MQ Adv. Zobrazení stavu nativních správců front HA pro kontejnery sestavené na míru

U vlastních kontejnerů můžete zobrazit stav nativních instancí vysoké dostupnosti pomocí příkazu **dspmq** .

Informace o této úloze

Pomocí příkazu **dspmq** můžete zobrazit provozní stav instance správce front v uzlu. Vrácené informace závisí na tom, zda je instance aktivní nebo zda je to replika. Informace poskytnuté aktivní instancí jsou konečné, informace z replikovaných uzlů mohou být zastaralé.

Můžete provést následující akce:

- Zobrazit, zda je instance správce front v aktuálním uzlu aktivní nebo zda je to replika.
- Zobrazit provozní stav nativní vysoké dostupnosti instance v aktuálním uzlu.
- Zobrazit provozní stav všech tří instancí v konfiguraci nativní vysoké dostupnosti.

Následující stavová pole se používají k hlášení stavu konfigurace nativní vysoké dostupnosti:

ROLE
Určuje aktuální roli instance a je jednou z hodnot `Active`, `Replica` nebo `Unknown`.

INSTANCE
Název poskytnutý pro tuto instanci správce front, když byl vytvořen pomocí volby **-lr** příkazu **crtmqm**.

INSYNC
Určuje, zda je instance v případě potřeby schopna převzít funkci aktivní instance.

QUORUM
Hlásí stav kvora ve formátu *počet_synchronizovaných_instancí*/*počet_nakonfigurovaných_instancí*.

REPLADDR
Adresa replikace instance správce front.

CONNACTV
Označuje, zda je uzel připojen k aktivní instanci.

BACKLOG
Označuje, kolik kB instance překročila.

CONNINST
Označuje, zda je pojmenovaná instance připojena k této instanci.

ALTDATE
Označuje datum, kdy byly tyto informace naposledy aktualizovány (prázdné, pokud dosud nebyly aktualizovány).

ALTTIME
Označuje čas poslední aktualizace těchto informací (prázdné, pokud dosud nebyla aktualizována).

Procedura

- Chcete-li určit, zda je instance správce front spuštěna jako aktivní instance nebo jako replika:

  ```
  dspmq -o status -m QMgrName
  ```

  Aktivní instance správce front s názvem BOB bude vykazovat následující stav:

  ```
  QMNAME(BOB)                STATUS(Running)
  ```

  Instance repliky správce front s názvem BOB bude vykazovat následující stav:

  ```
  QMNAME(BOB)                STATUS(Replica)
  ```

  Neaktivní instance bude hlásit následující stav:

  ```
  QMNAME(BOB)                STATUS(Ended Immediately)
  ```

- Chcete-li určit provozní stav nativní vysoké dostupnosti instance na aktuálním uzlu, postupujte takto:

  ```
  dspmq -o nativeha -m QMgrName
  ```

  Aktivní instance správce front s názvem BOB může vykazovat následující stav:

  ```
  QMNAME(BOB)              ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
  ```

  Instance repliky správce front s názvem BOB může vykazovat následující stav:

  ```
  QMNAME(BOB)              ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
  ```

  Neaktivní instance správce front s názvem BOB může vykazovat následující stav:

  ```
  QMNAME(BOB)              ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
  ```

- Chcete-li určit provozní stav nativní vysoké dostupnosti všech instancí v konfiguraci nativní vysoké dostupnosti:

  ```
  dspmq -o nativeha -x -m QMgrName
  ```

Pokud tento příkaz zadáte na uzlu, na kterém je spuštěna aktivní instance správce front BOB, můžete obdržet následující stav:

```
QMNAME(BOB)            ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

Pokud tento příkaz zadáte na uzlu, na kterém je spuštěna instance repliky správce front BOB, můžete obdržet následující stav, který znamená, že jedna z replik zaostává:

```
QMNAME(BOB)            ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(No)  BACKLOG(435)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

Pokud tento příkaz zadáte na uzlu, kde je spuštěna neaktivní instance správce front BOB, můžete obdržet následující stav:

```
QMNAME(BOB)            ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
 INSTANCE(inst1) ROLE(Unknown) REPLADDR(9.20.123.45) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst2) ROLE(Unknown) REPLADDR(9.20.123.46) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst3) ROLE(Unknown) REPLADDR(9.20.123.47) CONNACTV(No) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
```

Pokud zadáte příkaz, když se instance ještě domlouvají, která je aktivní a které jsou repliky, obdržíte následující stav:

```
QMNAME(BOB)              STATUS(Negotiating)
```

Související odkazy

dspmq (display queue managers) command

MQ Adv. Ukončení nativních správců front HA

Pomocí příkazu **endmqm** můžete ukončit aktivního nebo replikovaného správce front, který je součástí nativní skupiny HA.

Procedura

- Chcete-li ukončit aktivní instanci správce front, viz téma Ukončení nativních správců front HA v sekci Konfigurace v této dokumentaci.

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 Spojeného království ani jiných zemí, ve kterých je takovéto vyjádření v rozporu s místními zákony: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE "TAK, JAK 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. 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 interoperability softwaru, oddělení 49XA
3605 Dálnice 52 N

Rochester, MN 55901
U.S.A.

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

Licencovaný program popsaný v těchto informacích a veškerý licencovaný materiál, který je pro něj k dispozici, jsou poskytovány společností IBM na základě podmínek IBM Smlouvy se zákazníkem, IBM Mezinárodní licenční smlouvy pro programy 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 o programovacím rozhraní, jsou-li poskytnuty, jsou určeny k tomu, aby vám pomohly vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, která zákazníkům umožňují 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: Tyto informace o diagnostice, úpravách a ladění nepoužívejte jako programovací rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM , ibm.com, jsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek společnosti IBM je k dispozici na webu "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Další 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 zahrnuje software vyvinutý projektem Eclipse (https://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: