

7.5

*Plánování produktu IBM WebSphere MQ*

**IBM**

**Poznámka**

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí [“Poznámky” na stránce 153](#).

Toto vydání se vztahuje k verzi 7, vydání 5 produktu IBM® WebSphere MQ a ke všem následujícím vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak.

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

© **Copyright International Business Machines Corporation 2007, 2024.**

---

# Obsah

<b>Naplánování.....</b>	<b>5</b>
IBM MQ a IBM MQ Appliance místní aspekty připravenosti na GDPR.....	5
Návrh architektury IBM WebSphere MQ.....	14
Architektury jednotlivých správců front.....	14
Architektury jednotlivých správců front.....	15
Architektury jednotlivých správců front.....	15
Architektury jednotlivých správců front.....	15
Více architektur správce front.....	15
Dvoubodový systém zpráv.....	19
Úvod do publikování/odběru.....	19
Práce s nedoručené zprávy s manipulátorem fronty nedoručených zpráv.....	106
Plánování pro více instalací.....	115
Výběr primární instalace.....	116
Plánování vašich požadavků na ukládání a výkon.....	120
Požadavky na prostor na disku.....	121
Plánování podpory systému souborů.....	122
Zdroje pro produkt IBM WebSphere MQ a UNIX System V IPC.....	147
Sdílená paměť v systému AIX.....	148
Nastavení hodnot priority procesů systému UNIX.....	148
Plánování prostředí klienta IBM WebSphere MQ v systému HP Integrity NonStop Server.....	149
Příprava prostředí produktu HP Integrity NonStop Server.....	149
IBM WebSphere MQ a HP NonStop TMF.....	149
Použití HP NonStop TMF.....	150
<b>Poznámky.....</b>	<b>153</b>
Informace o programovacím rozhraní.....	154
Ochranné známky.....	154



# Naplánování

---

Při plánování vašeho prostředí IBM WebSphere MQ musíte vzít v úvahu architekturu IBM WebSphere MQ , kterou chcete konfigurovat, požadavky na prostředky, potřebu protokolování a zálohování. Pomocí odkazů v tomto tématu můžete naplánovat prostředí, v němž je produkt IBM WebSphere MQ spuštěn.

Než začnete plánovat své prostředí produktu IBM WebSphere MQ , seznamte se se základními koncepty produktu IBM WebSphere MQ , viz témata v tématu [Technický přehled](#).

## **Související pojmy**

[Dostupnost, obnova a restartování](#)

## **Související úlohy**

[Migrace](#)

[Instalace](#)

[Konfigurace](#)

[Správa produktu WebSphere MQ](#)

[Ujištění se, že zprávy nejsou ztraceny \(protokolování\)](#)

## **IBM MQ a IBM MQ Appliance místní aspekty připravenosti na GDPR**

---

### **Pro PID:**

- 5724-H72 IBM MQ
- 5655-AV9 IBM MQ Advanced pro z/OS
- 5655-AV1 IBM MQ Advanced for z/OS, Value Unit Edition
- 5655-AM9 IBM MQ Advanced Message Security for z/OS
- 5725-Z09 IBM MQ Appliance M2001
- 5725-S14 IBM MQ Appliance M2000
- 5655-MQ9 IBM MQ pro z/OS
- 5655-VU9 IBM MQ pro z/OS Value Unit Edition
- 5639-L92 IBM MQ Přímý průchod přes Internet
- 5655-MF9 IBM MQ Managed File Transfer pro z/OS
- 5655-ADV IBM WebSphere MQ Rozšířené pro z/OS
- 5655-AMS IBM WebSphere MQ Rozšířené zabezpečení zpráv pro systém z/OS
- 5724-R10 IBM WebSphere MQ File Transfer Edition for Multiplatforms (File Transfer Edition)
- 5724-A39 IBM WebSphere MQ pro server HP NonStop Server
- 5724-A38 IBM WebSphere MQ pro HP OpenVMS
- 5655-W97 IBM WebSphere MQ pro z/OS
- 5655-VU8 IBM WebSphere MQ pro z/OS Value Unit Edition
- 5655-VUE IBM WebSphere MQ pro z/OS Value Unit Edition
- 5725-C79 IBM WebSphere MQ Hypervisor Edition for Red Hat Enterprise Linux® for x86
- 5725-F22 IBM WebSphere MQ Hypervisor pro AIX
- 5655-MFT IBM WebSphere MQ Spravovaný přenos souborů pro z/OS

### **Upozornění:**

Tento dokument je zamýšlen jako pomoc při přípravě vaší připravenosti na GDPR. Poskytuje informace o funkcích produktu IBM MQ , které můžete konfigurovat, a o aspektech použití produktu, které byste

měli zvážit, abyste pomohli vaší organizaci s připraveností na GDPR. Tato informace není vyčerpávajícím seznamem z důvodu mnoha způsobů, jakým mohou klienti vybrat a konfigurovat funkce, a z širokého spektra způsobů, jak lze produkt použít samostatně a s aplikacemi a systémy třetích stran.

**Zákazníci jsou zodpovědní za zajištění vlastního dodržování různých zákonů a nařízení, včetně Obecného nařízení o ochraně osobních údajů Evropské unie. Zákazníci jsou výhradně odpovědní za získání poradenství příslušného právního poradce, pokud jde o identifikaci a výklad příslušných zákonů a předpisů, které mohou mít vliv na podnikání klientů, a jakékoli kroky, které mohou klienti potřebovat, aby dodržovali tyto zákony a předpisy.**

**Produkty, služby a ostatní funkce popsané v tomto dokumentu nejsou vhodné pro všechny situace klientů a mohou mít omezenou dostupnost. IBM neposkytuje právní, účetní ani auditorské rady ani neprohlašuje ani nezaručuje, že její služby či produkty zajistí, že zákazníci budou v souladu s jakýmkoli právními předpisy či nařízeními.**

## Obsah

1. [GDPR](#)
2. [Konfigurace produktu pro GDPR](#)
3. [Životní cyklus dat](#)
4. [Shromažďování dat](#)
5. [Ukládání dat](#)
6. [Přístup k datům](#)
7. [Zpracování dat](#)
8. [Odstranění dat](#)
9. [Monitorování dat](#)
10. [Funkce pro omezení používání osobních údajů](#)
11. [Obsluha souborů](#)

## GDPR

Obecné nařízení o ochraně osobních údajů (GDPR) bylo přijato Evropskou unií ("EU") a platí od 25. května 2018.

### Proč je důležité GDPR?

GDPR zavádí silnější regulační rámec pro ochranu dat ke zpracování osobních dat jednotlivců. GDPR přináší:

- Nová a rozšířená práva pro jednotlivce
- Rozšířená definice osobních dat
- Nové závazky pro procesory
- Potenciál významných finančních sankcí za nedodržování
- Povinná oznámení o narušení dat

### Přečtěte si více o GDPR:

- [Informační portál EU GDPR](#)
- [ibm.com/GDPR](http://ibm.com/GDPR) webové stránky

## Konfigurace produktu-aspekty připravenosti na GDPR

V následujících oddílech jsou uvedeny aspekty konfigurace produktu IBM MQ s cílem pomoci vaší organizaci s připraveností na GDPR.

## Životní cyklus dat

IBM MQ je transakční middlewarový produkt orientovaný na zprávy, který umožňuje aplikacím asynchronně vyměňovat data poskytovaná aplikacemi. IBM MQ podporuje řadu rozhraní API systému zpráv, protokolů a mostů pro účely připojení aplikací. Jako takový může být produkt IBM MQ použit k výměně mnoha forem dat, z nichž některé mohou být potenciálně předmětem GDPR. Existuje několik produktů třetích stran, s nimiž si může produkt IBM MQ vyměňovat data. Některé z nich jsou vlastněny společností IBM, ale mnoho dalších je poskytováno jinými dodavateli technologií. [Webové stránky sestav kompatibility softwarových produktů](#) poskytují seznamy přidruženého softwaru. Aspekty týkající se připravenosti produktu třetí strany na GDPR byste měli nahlédnout do dokumentace tohoto produktu. Administrátoři produktu IBM MQ řídí způsob, jakým produkt IBM MQ interaktivně spolupracuje s daty, která jím procházejí, pomocí definice front, témat a odběrů.

### Jaké typy datových toků procházejí produktem IBM MQ?

Vzhledem k tomu, že produkt IBM MQ poskytuje asynchronní službu systému zpráv pro data aplikace, neexistuje na tuto otázku žádná definitivní odpověď, protože případy použití se liší v závislosti na implementaci aplikace. Data zpráv aplikace jsou trvale uložena v souborech front (sady stránek nebo prostředek Coupling Facility v systému z/OS), protokoly a archivy a zpráva může obsahovat data, která řídí GDPR. Data zpráv poskytnutá aplikací mohou být také zahrnuta do souborů shromážděných pro účely určování problémů, jako jsou protokoly chyb, trasovací soubory a protokoly FFST. V aplikaci z/OS mohou být data zpráv zahrnuta také do adresního prostoru nebo výpisů paměti prostředku Coupling Facility.

Níže jsou uvedeny některé typické příklady osobních údajů, které lze vyměňovat pomocí produktu IBM MQ:

- Zaměstnanci zákazníka (například IBM MQ lze použít k připojení mzdových nebo personálních systémů zákazníka).
- Osobní údaje vlastních klientů zákazníka (například IBM MQ může zákazník použít k výměně dat mezi aplikacemi, které se vztahují k jeho klientům, například k převzetí obchodních příležitostí a ukládání dat v rámci jejich systému CRM).
- Citlivé osobní údaje zákazníků (například IBM MQ mohou být používány v oborových kontextech, které vyžadují výměnu osobních údajů, například HL7-based healthcare records při integraci klinických aplikací).

Kromě dat zpráv poskytnutých aplikací produkt IBM MQ zpracovává následující typy dat:

- Ověřovací pověření (například jméno uživatele a hesla, klíče rozhraní API atd.)
- Technicky identifikovatelné osobní údaje (například ID zařízení, identifikátory založené na použití, adresa IP atd. -ve spojení s jednotlivcem)

### Osobní údaje používané pro online kontakt s IBM

Klienti IBM MQ mohou odesílat online komentáře/zpětná vazba/požadavky na kontaktování IBM ohledně předmětů IBM MQ různými způsoby, především:

- Oblast veřejných komentářů na stránkách v oblasti [IBM MQ na webu IBM Developer](#)
- Oblast veřejných komentářů na stránkách informací o produktu [IBM MQ v produktu IBM Documentation](#)
- Veřejné komentáře ve fórech podpory [IBM](#)
- Veřejné komentáře v komunitě [IBM RFE na IBM Developer](#)

Obvykle se používá pouze jméno klienta a e-mailová adresa, aby se umožnilo osobní odpovědi pro předmět kontaktu a použití osobních údajů v souladu s [IBM Prohlášení o online ochraně osobních údajů](#).

## Shromažďování dat

IBM MQ lze použít ke shromažďování osobních dat. Při posuzování vašeho používání produktu IBM MQ a vašich potřeb vyhovět požadavkům GDPR byste měli zvážit typy osobních údajů, které za vašich okolností procházejí produktem IBM. Možná budete chtít zvážit aspekty, jako jsou:

- Jak data přicházejí do vašich správců front? (přes které protokoly? Jsou data šifrována? Jsou data podepsána?)
- Jak jsou data odesílána z vašich správců front? (přes které protokoly? Jsou data šifrována? Jsou data podepsána?)
- Jak jsou data ukládána při průchodu správcem front? (Každá aplikace systému zpráv má potenciál zapisovat data zpráv na stavová média, a to i v případě, že zpráva je dočasná. Víte, jak by funkce systému zpráv mohly potenciálně odhalit aspekty dat zpráv aplikace procházejících produktem?)
- Jak jsou pověření shromažďována a v případě potřeby ukládána produktem IBM MQ pro přístup k aplikacím třetích stran?

IBM MQ může vyžadovat komunikaci s jinými systémy a službami, které vyžadují ověření, například LDAP. V případě potřeby jsou ověřovací data (ID uživatelů, hesla) konfigurována a uložena produktem IBM MQ pro použití v takových komunikacích. Kdykoli je to možné, měli byste se vyvarovat použití osobních pověření pro ověření produktu IBM MQ. Zvažte ochranu úložiště použitého pro data ověření. (Viz níže uvedené datové úložiště.)

## Úložiště dat

Když data zpráv procházejí správcem front, produkt IBM MQ uchová (možná více kopií) tato data přímo na stavová média. Uživatelé produktu IBM MQ mohou zvážit zabezpečení dat zprávy v době, kdy jsou v klidu.

Následující položky zvýrazňují oblasti, ve kterých produkt IBM MQ trvale uchovává data poskytovaná aplikací, která mohou uživatelé zvážit při zajišťování shody s GDPR.

- Fronty zpráv aplikace:

IBM MQ poskytuje fronty zpráv, které umožňují asynchronní výměnu dat mezi aplikacemi. Dočasné a trvalé zprávy uložené ve frontě jsou zapisovány na stavová média.

- Fronty agenta přenosu souborů:

IBM MQ Managed File Transfer využívá fronty zpráv ke koordinaci spolehlivého přenosu dat souborů, soubory obsahující osobní data a záznamy přenosů jsou uloženy v těchto frontách.

- Přenosové fronty:

Pro spolehlivý přenos zpráv mezi správcem front jsou zprávy dočasně uloženy v přenosových frontách.

- Fronty nedoručených zpráv:

Za určitých okolností nemohou být zprávy vloženy do cílové fronty a jsou uloženy ve frontě nedoručených zpráv, pokud má správce front konfigurovanou frontu.

- Fronty vrácení:

Rozhraní systému zpráv JMS a XMS poskytují schopnost, která umožňuje přesunout nezpracovatelné zprávy do fronty vrácení poté, co došlo k několika vrácení, aby bylo možné zpracovat další platné zprávy.

- Fronta chyb AMS:

IBM MQ Advanced Message Security přesune zprávy, které nevyhovují zásadě zabezpečení, do SYSTEM.PROTECTION.ERROR.QUEUE je podobná frontě nedoručených zpráv.

- Zachovaná publikování:

Produkt IBM MQ poskytuje zachovanou funkci publikování, která odebírajícím aplikacím umožňuje odvolat předchozí publikaci.

Přečtěte si více:

- [Protokolování: Ujistěte se, že zprávy nejsou ztraceny](#)
- [Nastavení fronty agenta MFT](#)
- [Definování přenosové fronty](#)
- [Použití fronty nedoručených zpráv](#)
- [Obsluha nezpracovatelných zpráv ve třídách IBM MQ pro JMS](#)



- [Ošetření chyb AMS](#)
- [Zachovaná publikování](#)

Následující položky zvýrazňují oblasti, ve kterých může produkt IBM MQ nepřímo trvale uchovávat data, která mohou uživatelé zvážit při zajišťování shody s GDPR.

- **Systém zpráv trasy trasování:**

Produkt IBM MQ poskytuje funkce trasování trasy, které zaznamenávají trasu, kterou má zpráva mezi aplikacemi. Generované zprávy událostí mohou zahrnovat technicky identifikovatelné osobní údaje, jako jsou adresy IP.

- **Trasování aktivity aplikace:**

IBM MQ poskytuje trasování aktivity aplikace, které zaznamenává aktivity rozhraní API systému zpráv aplikací a kanálů. Trasování aktivity aplikace může zaznamenávat obsah dat zpráv poskytnutých aplikací do zpráv událostí.

- **Trasování služby:**

Produkt IBM MQ poskytuje funkce trasování služeb, které zaznamenávají cesty interního kódu, jimiž prochází datové toky zpráv. V rámci těchto funkcí může produkt IBM MQ zaznamenávat obsah dat zpráv poskytnutých aplikací do trasovacích souborů uložených na disku.

- **Události správce front:**

IBM MQ může generovat zprávy událostí, které mohou zahrnovat osobní data, jako jsou události oprávnění, příkazy a konfigurace.

Přečtěte si více:

- [Trasovat-směrování zpráv](#)
- [Použití trasování](#)
- [Monitorování událostí](#)
- [Události správce front](#)

Chcete-li chránit přístup ke kopiím dat zpráv poskytnutých aplikací, zvažte následující akce:

- Omezte přístup oprávněného uživatele k datům IBM MQ v systému souborů, například omezte členství uživatele ve skupině 'mqm' na platformách UNIX .
- Omezte přístup aplikací k datům produktu IBM MQ prostřednictvím vyhrazených front a řízení přístupu. V případě potřeby se vyhněte zbytečnému sdílení prostředků, jako jsou fronty mezi aplikacemi, a poskytněte podrobné řízení přístupu k prostředkům front a témat.
- Produkt IBM MQ Advanced Message Security poskytuje komplexní podepisování a/nebo šifrování dat zpráv.
- K ochraně obsahu adresáře použitého k ukládání protokolů trasování použijte šifrování na úrovni souboru nebo svazku.
- Po odeslání trasování služby do produktu IBM MQ můžete odstranit soubory trasování služby a data FFST, pokud máte obavy o obsah potenciálně obsahující osobní data.

Přečtěte si více:

- [Oprávnění uživatelé](#)
- [Plánování podpory systému souborů na platformě Multiplatforms](#)

Administrátor produktu IBM MQ může nakonfigurovat správce front s pověřeními (jméno uživatele a heslo, klíče rozhraní API atd.) pro 3rd , jako např. LDAP, IBM Cloud Product Insights, Salesforce atd. Tato data jsou obecně uložena v datovém adresáři správce front chráněném prostřednictvím oprávnění systému souborů.

Při vytvoření správce front IBM MQ je datový adresář nastaven s řízením přístupu založeným na skupinách tak, aby produkt IBM MQ mohl číst konfigurační soubory a používat pověření pro připojení k těmto systémům. IBM MQ Administrátoři jsou považováni za oprávněné uživatele a jsou členy této skupiny, takže

mají přístup pro čtení k souborům. Některé soubory jsou zamlžené, ale nejsou šifrované. Z tohoto důvodu byste měli zvážit následující akce, abyste plně ochránili přístup k pověřením:

- Omezte přístup oprávněného uživatele k datům produktu IBM MQ , například omezte členství ve skupině 'mqm' na platformách UNIX .
- K ochraně obsahu datového adresáře správce front použijte šifrování na úrovni souboru nebo svazku.
- Šifrujte zálohy produkčního konfiguračního adresáře a uložte je s příslušným řízením přístupu.
- Zvažte poskytnutí záznamů auditu pro selhání ověření, řízení přístupu a změny konfigurace s událostmi zabezpečení, příkazů a konfigurace.

Přečtěte si více:

- [Zabezpečení IBM MQ](#)

## Přístup k datům

K datům správce front IBM MQ lze přistupovat prostřednictvím následujících rozhraní produktu, z nichž některá jsou určena pro přístup prostřednictvím vzdáleného připojení a jiná pro přístup prostřednictvím lokálního připojení.

- IBM MQ Konzola [ pouze vzdálená]
- IBM MQ Rozhraní REST API [ pouze vzdálené]
- MQI [ Lokální a vzdálený]
- JMS [ Lokální a vzdálený]
- XMS [ Lokální a vzdálený]
- IBM MQ Telemetrie (MQTT) [ pouze vzdálená]
- IBM MQ Light (AMQP) [ pouze vzdálené]
- IBM MQ IMS [ Pouze lokální]
- IBM MQ CICS bridge [ pouze lokální]
- IBM MQ most pro HTTP [ pouze vzdálený]
- IBM MQ Mosty protokolu MFT [ pouze vzdálené]
- IBM MQ Connect:Direct mosty [ pouze vzdálené]
- IBM MQ Bridge to Salesforce [ Pouze vzdálený]
- IBM MQ Bridge to Blockchain [ Pouze vzdálený]
- IBM MQ MQAI [ lokální a vzdálený]
- IBM MQ Příkazy PCF [ Lokální a vzdálené]
- IBM MQ Příkazy MQSC [ Lokální a vzdálené]
- IBM MQ Průzkumník [ Lokální a vzdálený]

Rozhraní jsou navržena tak, aby uživatelům umožnila provádět změny ve správci front IBM MQ a ve zprávách, které jsou v něm uloženy. Operace správy a zasilání zpráv jsou zabezpečeny tak, aby byly při podání žádosti zapojeny tři fáze;

- Ověřování
- Mapování rolí
- Autorizace

### Ověřování:

Pokud byla zpráva nebo administrativní operace vyžádána z lokálního připojení, zdrojem tohoto připojení je spuštěný proces na stejném systému. Uživatel, který spustil proces, musí projít všemi kroky ověření poskytnutými operačním systémem. Jméno uživatele vlastníka procesu, ze kterého bylo vytvořeno připojení, je deklarována jako identita. Může se jednat například o jméno uživatele, který spustil shell, ze kterého byla spuštěna aplikace. Možné formy ověřování pro lokální připojení jsou:

1. Deklarovaný název uživatele (lokální OS)
2. Volitelné jméno uživatele a heslo (OS, LDAP nebo vlastní 3rd stran)

Pokud byla administrativní akce vyžádána ze vzdáleného připojení, provede se komunikace s produktem IBM MQ prostřednictvím síťového rozhraní. Následující formy identity mohou být předloženy k ověření prostřednictvím síťových připojení;

1. Deklarovaný název uživatele (ze vzdáleného operačního systému)
2. Jméno uživatele a heslo (OS, LDAP nebo vlastní 3rd stran)
3. Zdrojová síťová adresa (například adresa IP)
4. X.509 Digitální certifikát (vzájemné ověření SSL/TLS)
5. Tokeny zabezpečení (například token LTPA2).
6. Další vlastní zabezpečení (schopnost poskytovaná 3rd stranami)

### **Mapování rolí:**

Ve fázi mapování rolí mohou být pověření poskytnutá ve fázi ověřování mapována na alternativní identifikátor uživatele. Za předpokladu, že je povoleno pokračovat v mapování identifikátoru uživatele (například administrativní uživatelé mohou být blokováni pravidly ověřování kanálu), bude mapované ID uživatele přeneseno do konečné fáze při autorizaci aktivit vůči prostředkům produktu IBM MQ.

### **Autorizace:**

Produkt IBM MQ poskytuje různým uživatelům možnost mít různá oprávnění pro různé prostředky systému zpráv, jako jsou fronty, témata a další objekty správce front.

### **Protokolování aktivity:**

Někteří uživatelé produktu IBM MQ mohou potřebovat vytvořit záznam auditu o přístupu k prostředkům produktu MQ. Příklady požadovaných protokolů auditu mohou zahrnovat změny konfigurace, které obsahují informace o změně kromě toho, kdo ji požadoval.

K implementaci tohoto požadavku jsou k dispozici následující zdroje informací:

1. Správce front IBM MQ lze nakonfigurovat tak, aby vytvářel události příkazů po úspěšném spuštění příkazu administrátora.
2. Správce front IBM MQ lze konfigurovat pro vytváření událostí konfigurace při vytváření, změně nebo odstranění prostředku správce front.
3. Správce front IBM MQ lze konfigurovat tak, aby generoval událost oprávnění v případě selhání kontroly autorizace prostředku.
4. Do protokolů chyb správce front se zapisují chybové zprávy označující, že se nezdařily kontroly autorizace.
5. Webová konzola IBM MQ zapíše zprávy auditu do svých protokolů při selhání ověření, kontrol autorizace nebo při vytvoření, spuštění, zastavení či odstranění správců front.

Při zvažování tohoto druhu řešení mohou uživatelé produktu IBM MQ zvážit následující aspekty:

- Zprávy událostí jsou dočasné, takže když správce front restartuje, dojde ke ztrátě informací. Všechny monitory událostí by měly být konfigurovány tak, aby neustále spotřebovávaly všechny dostupné zprávy a přenášovaly obsah na trvalá média.
- IBM MQ privilegovaní uživatelé mají dostatečná oprávnění pro zakázání událostí, vymazání protokolů nebo odstranění správců front.

Další informace o zabezpečení přístupu k datům produktu IBM MQ a poskytnutí záznamu pro audit viz následující témata:

- [IBM MQ mechanizmy zabezpečení](#)
- [Události konfigurace](#)
- [Události příkazů](#)
- [Protokoly chyb](#)

## Zpracování dat

### Šifrování pomocí infrastruktury veřejných klíčů:

Můžete zabezpečit síťová připojení k produktu IBM MQ pro použití TLS, což může také poskytnout vzájemné ověření inicializační strany připojení.

Použití prostředků zabezpečení PKI poskytovaných mechanismy přenosu je prvním krokem k zabezpečení zpracování dat pomocí produktu IBM MQ. Avšak bez povolení dalších funkcí zabezpečení je chování přijímající aplikace zpracovat všechny zprávy, které jí byly doručeny, bez ověření původu zprávy nebo bez toho, zda byla během přenosu změněna.

Uživatelé produktu IBM MQ, kteří jsou licencováni pro použití funkcí Advanced Message Security (AMS), mohou řídit způsob, jakým aplikace zpracovávají osobní data uchovávaná ve zprávách, prostřednictvím definice a konfigurace zásad zabezpečení. Zásady zabezpečení umožňují použití digitálního podepisování a/nebo šifrování pro data zpráv mezi aplikacemi.

Je možné použít zásady zabezpečení, které vyžadují a ověřují digitální podpis, když spotřebovávají zprávy, aby se zajistilo, že jsou zprávy autentické. Šifrování AMS poskytuje metodu, kterou se data zpráv převádějí z čitelné podoby na kódovanou verzi, kterou může dekódovat pouze jiná aplikace, pokud je to zamýšlený příjemce nebo zpráva a má přístup ke správnému dešifrovacímu klíči.

Další informace o použití zabezpečení SSL a certifikátů k zabezpečení síťových připojení naleznete v následujících tématech v dokumentaci k produktu IBM MQ V9 :

- [Konfigurace zabezpečení TLS pro IBM MQ](#)
- [Přehled AMS](#)

### Odstranění dat

IBM MQ poskytuje příkazy a akce uživatelského rozhraní pro odstranění dat, která byla poskytnuta produktu. To umožňuje uživatelům produktu IBM MQ s prostředky odstranit data, která se vztahují k určitým jednotlivcům, v případě potřeby.

- Oblasti chování produktu IBM MQ, které je třeba zvážit pro splnění požadavků na odstranění dat klienta GDPR
  - Odstranit data zpráv uložená ve frontě aplikací pomocí:
    - Odebrání jednotlivých zpráv pomocí rozhraní API systému zpráv nebo nástrojů nebo pomocí vypršení platnosti zpráv.
    - Určení, že zprávy jsou dočasné a jsou uloženy ve frontě, kde je třída přechodných zpráv normální, a restartování správce front.
    - Administrativní vymazání fronty.
    - Odstranění fronty.
  - Odstranit zachovaná data publikování uložená v tématu pomocí:
    - Určení, že zprávy jsou dočasné, a restartování správce front.
    - Nahrazení uchovaných dat novými daty nebo pomocí vypršení platnosti zprávy.
    - Administrativní vymazání řetězce tématu.
  - Odstraňte data uložená ve správci front odstraněním celého správce front.
  - Odstraňte data uložená příkazy trasování služby tak, že odstraníte soubory v adresáři trasování.
  - Odstraňte data FFST uložená odstraněním souborů v adresáři chyb.
  - Odstraňte adresní prostor a výpisy paměti prostředku Coupling Facility (v systému z/OS).
  - Odstraňte archivní, záložní nebo jiné kopie těchto dat.
- Oblasti chování produktu IBM MQ, které je třeba zvážit pro splnění požadavků na odstranění dat účtu GDPR

- Data účtu a předvolby uložené produktem IBM MQ pro připojení ke správcům front a službám strany 3rd můžete odstranit odstraněním (včetně jejich archivních, záložních nebo jinak replikovaných kopií):
  - Objekty ověřovacích informací správce front, které ukládají pověření.
  - Záznamy oprávnění správce front, které odkazují na identifikátory uživatelů.
  - Pravidla ověřování kanálu správce front, která mapují nebo blokují specifické adresy IP, DN certifikátu nebo identifikátory uživatelů.
  - Soubory pověření používané produktem IBM MQ Managed File Transfer Agent, Logger a MQ Explorer MFT Plugin pro ověření se správcem front a souborovým serverem.
  - X.509 digitální certifikáty, které představují nebo obsahují informace o jednotlivci z úložišť klíčů, které mohou být použity pomocí připojení SSL/TLS nebo IBM MQ Advanced Message Security (AMS).
  - Individuální uživatelské účty ze zařízení IBM MQ Appliance, včetně odkazu na tyto účty v souborech systémového protokolu.
  - IBM MQ Metadata pracovního prostoru průzkumníka a nastavení Eclipse .
  - IBM MQ Úložiště hesel Průzkumníka, jak je uvedeno v [Předvolbách hesla](#).
  - IBM MQ Konfigurační soubory konzoly a serveru mqweb.
  - Konfigurační soubory dat připojení Salesforce .
  - Konfigurační soubory dat připojení blockchain.
  - IBM Cloud Product Insights data připojení v sekci ReportingService v qm.ini a APIKeyFile.

Přečtěte si více:

- [Konfigurace produktu IBM MQ Bridge to Salesforce](#)
- [Konfigurace produktu IBM MQ pro použití s technologií blockchain](#)
- [MFT a IBM MQ ověření připojení](#)
- [Mapování pověření pro souborový server pomocí souboru ProtocolBridgeCredentials.xml](#)
- [Konfigurace IBM MQ Uživatelé a role konzoly](#)

## Monitorování dat

Produkt IBM MQ poskytuje řadu funkcí monitorování, které mohou uživatelé využít k lepšímu pochopení výkonu aplikací a správců front.

Produkt IBM MQ také poskytuje řadu funkcí, které pomáhají spravovat protokoly chyb správce front.

Přečtěte si více:

- [Monitorování sítě IBM MQ](#)
- [Služby zpráv diagnostiky](#)
- [QMErrorLog](#)

IBM MQ poskytuje funkci, která uživatelům umožňuje publikovat informace ve službě IBM Cloud Product Insights , aby uživatel IBM MQ mohl zobrazit informace o spuštění a použití správce front.

Přečtěte si více:

- [Konfigurace produktu IBM MQ pro použití se službou IBM Cloud Product Insights v produktu IBM Cloud](#)

## Schopnost omezovat používání osobních údajů

Pomocí prostředků shrnutých v tomto dokumentu produkt IBM MQ umožňuje koncovému uživateli omezit použití jeho osobních údajů.

IBM MQ fronty zpráv by neměly být používány jako trvalé datové úložiště stejným způsobem jako databáze, což platí zejména při zpracování dat aplikace, na která se vztahuje GDPR.

Na rozdíl od databáze, kde mohou být data nalezena prostřednictvím dotazu hledání, může být obtížné najít data zprávy, pokud neznáte frontu, identifikátory zprávy a korelace zprávy.

Za předpokladu, že zprávy obsahující data jednotlivce lze snadno identifikovat a vyhledat, je možné použít standardní funkce systému zpráv IBM MQ pro přístup k datům zpráv nebo pro jejich úpravu.

## Zpracování souborů

1. IBM MQ Managed File Transfer neprovádí skenování malwaru na přenesených souborech. Soubory se přenášejí tak, jak jsou, a provádí se kontrola integrity, aby se zajistilo, že data souboru nebudou během přenosu upravena. Kontrolní součty zdroje a cíle jsou publikovány jako součást publikování stavu přenosu. Doporučuje se, aby koncoví uživatelé implementovali skenování malwaru podle potřeby pro své prostředí před tím, než MFT přeneše soubor a poté, co MFT doručí soubor do vzdáleného koncového bodu.
2. IBM MQ Managed File Transfer neprovádí akce na základě typu MIME nebo přípony souboru. MFT čte soubory a přenáší bajty přesně tak, jak byly načteny ze vstupního souboru.

## Návrh architektury produktu IBM WebSphere MQ

---

Zjistěte si informace o různých architekturách, které produkt IBM WebSphere MQ podporuje pro styly systému zpráv typu point-to-point a publikování/odběr.

Před plánováním architektury produktu IBM WebSphere MQ se seznamte se základními koncepty produktu IBM WebSphere MQ, viz témata v tématu [IBM WebSphere MQ Technical overview](#).

IBM WebSphere MQ architektury sahají od jednoduchých architektur pomocí jediného správce front až po složitější sítě vzájemně propojených správců front. Několik správců front je propojeno pomocí distribuovaných technik použití front. Další informace o plánování jednotlivých správců front a vícearchitekturách správců front naleznete v následujících tématech:

- [“Architektury založené na jednom správci front”](#) na stránce 14
- [“Architektury založené na více správcích front”](#) na stránce 15
- [“Sítě a síťové plánování”](#) na stránce 16
- [Techniky distribuovaného systému zpráv produktu WebSphere MQ](#)

Potřebujete-li více správců front, kteří logicky souvisí a potřebují sdílet data a aplikace, mohou být seskupeny v klastru. Pomocí klastrů můžete povolit správcům front vzájemnou komunikaci bez nutnosti nastavit další definice kanálů nebo definice vzdálených front, a zjednodušit tak jejich konfiguraci a správu. Další informace o použití klastrů najdete v tématu [Jak klastry fungují](#).

### Související pojmy

[“Naplánování”](#) na stránce 5

Při plánování vašeho prostředí IBM WebSphere MQ musíte vzít v úvahu architekturu IBM WebSphere MQ, kterou chcete konfigurovat, požadavky na prostředky, potřebu protokolování a zálohování. Pomocí odkazů v tomto tématu můžete naplánovat prostředí, v němž je produkt IBM WebSphere MQ spuštěn.

### Související úlohy

[Konfigurace](#)

## Architektury založené na jednom správci front

Nejjednodušší IBM WebSphere MQ architektury zahrnují konfiguraci a použití jednoho správce front.

Před plánováním architektury produktu IBM WebSphere MQ se seznamte se základními koncepty produktu IBM WebSphere MQ, viz téma [Úvod do produktu IBM WebSphere MQ](#).

Několik možných architektur používajících jediného správce front je popsáno v následujících sekcích:

- [“Jednotlivý správce front s lokálními aplikacemi, které přistupují ke službě”](#) na stránce 15
- [“Jediný správce front se vzdálenými aplikacemi, které přistupují ke službě jako klienti”](#) na stránce 15

- [“Jednotlivý správce front s konfigurací publikování/odběru”](#) na stránce 15

## Jednotlivý správce front s lokálními aplikacemi, které přistupují ke službě

První architektura založená na jediném správci front, je místo, kde aplikace přistupující ke službě běží na stejném systému jako aplikace poskytující službu. Správce front produktu IBM WebSphere MQ poskytuje asynchronní vzájemnou komunikaci mezi aplikacemi, které vyžadují službu, a aplikací, které tuto službu poskytují. To znamená, že komunikace mezi aplikacemi může pokračovat i v případě, že jedna z aplikací je ve stavu offline po delší dobu.

## Jediný správce front se vzdálenými aplikacemi, které přistupují ke službě jako klienti

Druhá architektura založená na jediném správci front má aplikace spuštěné vzdáleně z aplikací poskytujících službu. Vzdálené aplikace jsou spuštěny na různých systémech pro služby. Aplikace se připojují jako klienti k jednomu správci front. To znamená, že přístup ke službě může být poskytován více systémům prostřednictvím jediného správce front.

Omezení této architektury spočívá v tom, že musí být k dispozici síťové připojení pro aplikaci, která má fungovat. Interakce mezi aplikací a správcem front přes síťové připojení je synchronní.

## Jednotlivý správce front s konfigurací publikování/odběru

Alternativní architekturou, která používá jednoho správce front, je použití konfiguraci publikování/odběru. V systému zpráv typu publikování/odběr můžete oddělit poskytovatele informací od spotřebitelů dané informace. Liší se od bodu k bodového stylu systému zpráv v dříve popsanych architekturách, kde aplikace musí znát informace o cílové aplikaci, například název fronty, na které se mají zprávy vkládat. Při použití IBM WebSphere MQ publish/subscribe bude odesílající aplikace publikovat zprávu s uvedeným tématem na základě předmětu informací. Produkt IBM WebSphere MQ zpracovává distribuci zprávy aplikacím, které zaregistrovaly zájem o toto téma prostřednictvím odběru. Přijímající aplikace také nepotřebují vědět nic o zdroji zpráv, které mají být přijímány. Další informace o systému zpráv publikování/odběru naleznete v části Úvod do systému zpráv publikování a odběru produktu WebSphere MQ. Příklad systému zpráv publikování/odběru pomocí jednoho správce front naleznete v tématu [Příklad konfigurace publikování/odběru jednoho správce front](#).

### Související pojmy

[“Návrh architektury produktu IBM WebSphere MQ”](#) na stránce 14

Zjistěte si informace o různých architekturách, které produkt IBM WebSphere MQ podporuje pro styly systému zpráv typu point-to-point a publikování/odběr.

### Související informace

[Úvod do produktu WebSphere MQ](#)

[Vytváření a údržba správců front](#)

## Architektury založené na více správcích front

Distribuované techniky front zpráv můžete použít k vytvoření architektury produktu IBM WebSphere MQ zahrnující konfiguraci a použití více správců front.

Před plánováním architektury produktu IBM WebSphere MQ se seznamte se základními koncepty produktu IBM WebSphere MQ, viz téma [Úvod do produktu IBM WebSphere MQ](#).

Architektura IBM WebSphere MQ může být změněna bez změny aplikací, které poskytují služby, přidáním dalších správců front.

Aplikace mohou být hostovány na stejném počítači jako správce front a poté mohou získat asynchronní komunikaci se službou hostovanou na jiném správci front na jiném systému. Nebo aplikace přistupující ke službě se mohou připojit jako klienti ke správci front, který pak poskytuje asynchronní přístup ke službě v jiném správci front.



Přenosové cesty, které spojují různé správce front a jejich fronty, jsou definovány pomocí technik distribuovaných front. Správci front v rámci architektury jsou připojeni pomocí kanálů. Kanály se používají k automatickému přesouvání zpráv z jednoho správce front do jiného v jednom směru v závislosti na konfiguraci správců front.

Informace o vysoké úrovni pro plánování sítě IBM WebSphere MQ naleznete v příručce [“Sítě a síťové plánování”](#) na stránce 16.

Informace o způsobu plánování kanálů pro architekturu IBM WebSphere MQ naleznete v příručce [WebSphere MQ distributed-messaging techniques](#).

Distribuovaná správa front vám umožňuje vytvářet a monitorovat komunikaci mezi správci front. Další informace o distribuované správě front najdete v tématu [Úvod do distribuované správy front](#).

### **Související pojmy**

[Úvod do produktu WebSphere MQ](#)

[“Návrh architektury produktu IBM WebSphere MQ”](#) na stránce 14

Zjistěte si informace o různých architekturách, které produkt IBM WebSphere MQ podporuje pro styly systému zpráv typu point-to-point a publikování/odběr.

### **Související úlohy**

[Vytváření a údržba správců front](#)

## **Sítě a síťové plánování**

Produkt WebSphere MQ odesílá a přijímá data mezi aplikacemi a přes síť s použitím správců front a kanálů. Plánování sítě zahrnuje definování požadavků na vytvoření rámce pro připojení těchto systémů po síti.

Kanály lze vytvořit mezi vaším systémem a libovolným jiným systémem, se kterým potřebujete mít komunikaci. Vícepřechodové kanály lze vytvořit pro připojení k systémům, kde nemáte žádná přímá připojení. Připojení kanálu zpráv popsaná ve scénářích se zobrazují jako síťový diagram v produktu [Obrázek 1](#) na stránce 17.

## **Názvy kanálů a přenosových front**

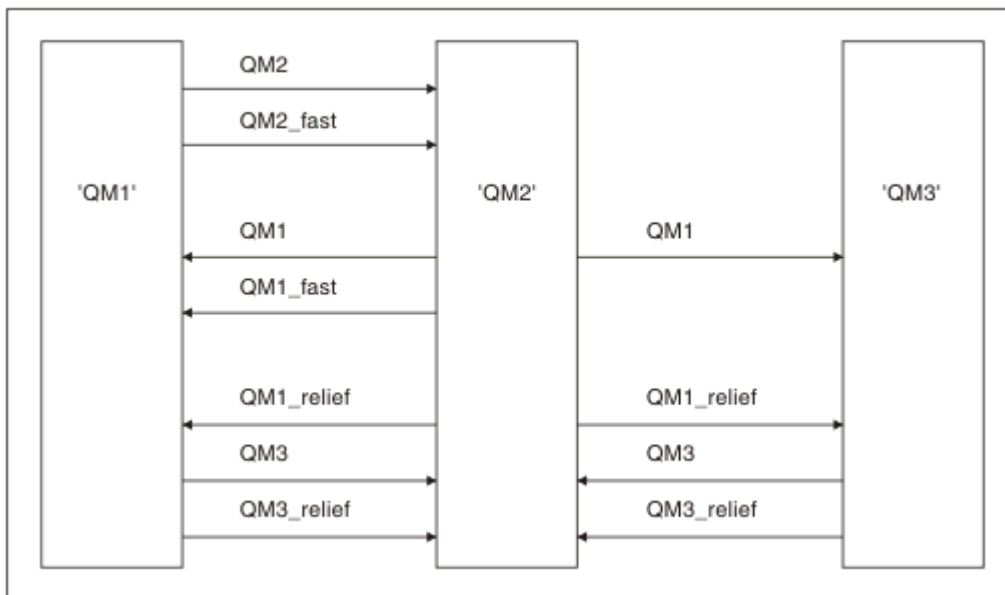
Přenosovým frontám může být přidělen libovolný název. Aby se však předešlo nejasnostem, můžete jim podle potřeby zadat stejné názvy jako názvy správce cílové fronty nebo názvy alias správce front. To asociuje přenosovou frontu s trasou, kterou používají, což poskytuje jasný přehled paralelních tras vytvořených zprostředkujícími správci front (s více přestrojeními).

Pro názvy kanálů není to tak clear-cut. Názvy kanálů v produktu [Obrázek 1](#) na stránce 17 pro QM2, například, musí být odlišné pro příchozí a odchozí kanály. Všechny názvy kanálů mohou stále obsahovat názvy jejich přenosových front, ale musí být kvalifikovány, aby je bylo možné je označit jako jedinečné.

Například v QM2 existuje kanál QM3 pocházející z QM1a kanál QM3 do systému QM3. Chcete-li, aby názvy byly jedinečné, první může mít název 'QM3\_from\_QM1' a druhý název může mít název 'QM3\_from\_QM2'. Tímto způsobem názvy kanálů zobrazují název přenosové fronty v první části názvu. Směr a sousedící název správce front jsou zobrazeny v druhé části názvu.

Tabulka doporučených názvů kanálů pro produkt [Obrázek 1](#) na stránce 17 je uvedena v produktu [Tabulka 1](#) na stránce 17.





Obrázek 1. Diagram sítě zobrazující všechny kanály

Tabulka 1. Příklad názvů kanálů

Název trasy	Správci front-kanál hostování	Jméno přenosové fronty	Doporučený název kanálu
QM1	QM1 & QM2	QM1 (na QM2)	QM1.from.QM2
QM1	QM2 & QM3	QM1 (na QM3)	QM1.from.QM3
QM1_fast	QM1 & QM2	QM1_fast (na QM2)	QM1_fast.from.QM2
QM1_relief	QM1 & QM2	QM1_relief (na QM2)	QM1_relief.from.QM2
QM1_relief	QM2 & QM3	QM1_relief (na QM3)	QM1_relief.from.QM3
QM2	QM1 & QM2	QM2 (na QM1)	QM2.from.QM1
QM2_fast	QM1 & QM2	QM2_fast (na QM1)	QM2_fast.from.QM1
QM3	QM1 & QM2	QM3 (na QM1)	QM3.from.QM1
QM3	QM2 & QM3	QM3 (na QM2)	QM3.from.QM2
QM3_relief	QM1 & QM2	QM3_relief (na QM1)	QM3_relief.from.QM1
QM3_relief	QM2 & QM3	QM3_relief (v QM2)	QM3_relief.from.QM2

**Poznámka:**

1. V produktu WebSphere MQ for z/OS jsou názvy správců front omezeny na čtyři znaky.
2. Pojmenujte všechny kanály v síti jedinečně. Jak je zobrazeno v části [Tabulka 1 na stránce 17](#), včetně názvů zdrojového a cílového správce front v názvu kanálu je dobrý způsob, jak to provést.

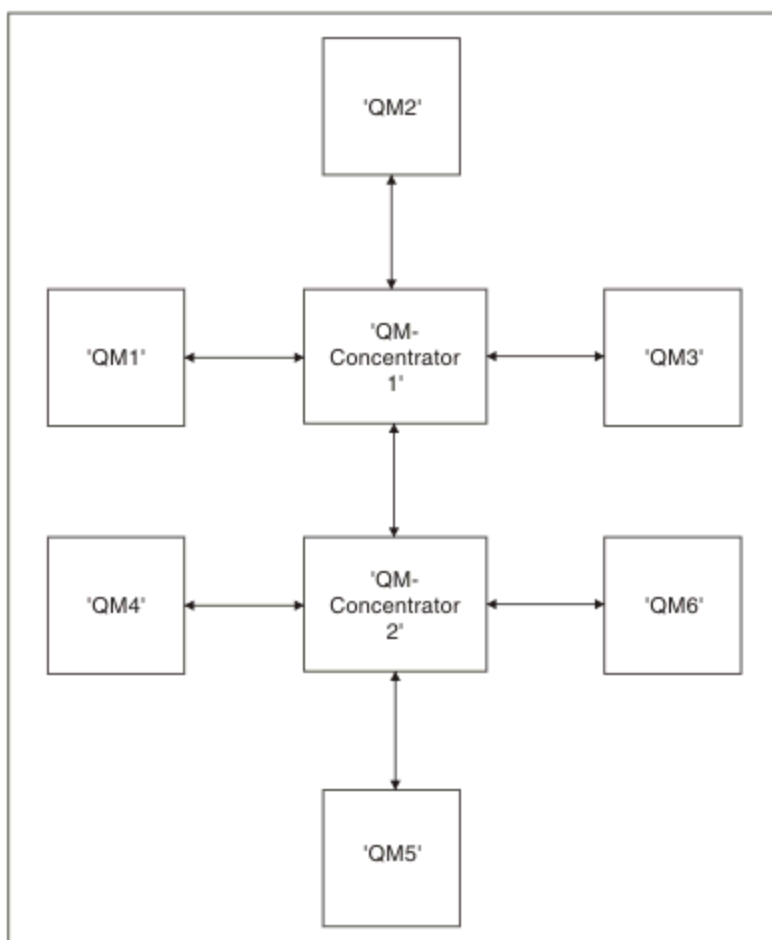
**Plánovač sítě**

Vytvoření sítě předpokládá, že existuje další, vyšší úroveň funkce *plánovače sítě*, jejíž plány jsou implementovány ostatními členy týmu.

U široce používaných aplikací je hospodárnější přemýšlet o lokálních přístupových místech pro koncentraci přenosu zpráv pomocí širokopásmových propojení mezi místními přístupovými servery, jak je zobrazeno v Obrázek 2 na stránce 18.

V tomto příkladu jsou dva hlavní systémy a řada satelitních systémů. Skutečná konfigurace by závisela na obchodních aspektech. K dispozici jsou dva správci front koncentrátoru umístěnými v levhodných centrech. Každý produkt QM-concentrator má kanály zpráv pro lokální správce front:

- QM-koncentrátor 1 má kanály zpráv pro každý ze tří lokálních správců front, QM1, QM2a QM3. Aplikace, které používají tyto správce front, mohou mezi sebou komunikovat prostřednictvím koncentrátorů QM-concentrators.
- Aplikace QM-concentrator 2 má kanály zpráv pro každý ze tří lokálních správců front, QM4, QM5a QM6. Aplikace, které používají tyto správce front, mohou mezi sebou komunikovat prostřednictvím koncentrátorů QM-concentrators.
- Aplikace QM-concentrators mají kanály zpráv mezi sebou tak, že každá aplikace ve správci front umožňuje výměnu zpráv s libovolnou jinou aplikací v jiném správci front.



Obrázek 2. Diagram sítě ukazující QM-koncentrátory

## Klastrování

Toto téma obsahuje pokyny pro plánování a administraci klastrů IBM WebSphere MQ . Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

Následující informace předpokládají, že uživatel má základní informace o klastrech produktu IBM WebSphere MQ . Tyto informace nejsou zamýšleny jako "jedna velikost pro všechny" řešení, ale snaží se sdílet společné přístupy ke společným problémům.

Klastry poskytují mechanismus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci požadovanou pro nastavení systému a požadovanou průběžnou správu. Čím větší je konfigurace, tím větší je výhoda.

Je třeba věnovat pozornost plánování klastrovaných systémů, aby se zajistilo, že fungují správně a zajišťují úroveň dostupnosti a reakční schopnosti požadované systémem, zejména u větších nebo složitějších klastrovaných systémů.

Úspěšné nastavení klastru závisí na dobrém plánování a důkladném pochopení základních principů produktu IBM WebSphere MQ, jako je například kvalitní správa aplikací a návrh sítě. Ujistěte se, že jste obeznámeni s informacemi v tématu [Koncepte vzájemné komunikace](#) a [Jak fungují klastry](#).

## Co jsou klastry a proč se používají?

Klastrování poskytuje dva klíčové výhody:

- Klastry zjednodušují administraci sítí IBM WebSphere MQ, které obvykle vyžadují konfiguraci mnoha definic objektů pro kanály, vysílací fronty a vzdálené fronty. Tato situace je zvláště pravdivá ve velkých, potenciálně měnících se sítích, v nichž je třeba vzájemně propojit mnoho správců front. Tato architektura je obzvláště těžká pro konfiguraci a aktivní údržbu.
- Klastry lze použít k rozdělení pracovní zátěže provozu zpráv mezi frontami a správci front v klastru. Taková distribuce umožňuje rozdělení pracovní zátěže zpráv jedné fronty na ekvivalentní instance této fronty umístěné ve více správcích front. Toto rozdělení pracovní zátěže lze použít k dosažení větší odolnosti vůči selháním systému a ke zlepšení výkonu škálování u zvláště aktivních toků zpráv v systému. V takovém prostředí má každá z instancí distribuovaných front aplikace, které zpracovávají zprávy.

### Související informace

[Klastrování: doporučené postupy](#)

## Dvoubodový systém zpráv

Nejjednodušší formou systému zpráv v produktu IBM WebSphere MQ je systém zpráv typu point-to-point.

V systému zpráv typu point-to-point musí odesílající aplikace znát informace o přijímající aplikaci před tím, než může odeslat zprávu do této aplikace. Odesílající aplikace může například potřebovat znát název fronty, do níž se mají odeslat informace, a může také zadat název správce front.

Alternativní styl systému zpráv, který můžete použít s produktem IBM WebSphere MQ, je systém zpráv typu publikování/odběr. Systém zpráv typu publikování/odběr vám umožňuje oddělit poskytovatele informací od spotřebitelů těchto informací. Odesílající aplikace a přijímající aplikace nemusí o sobě vědět nic o tom, které informace mají být odeslány a přijaty. Další informace o systému zpráv publikování/odběru naleznete v části [Úvod do systému zpráv publikování a odběru produktu WebSphere MQ](#).

### Související informace

[Vývoj aplikací](#)

[Zprávy produktu WebSphere MQ](#)

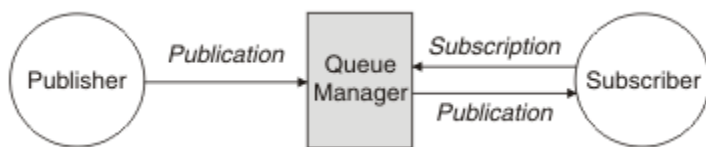
## Úvod do systému zpráv publikování/odběru produktu IBM WebSphere MQ

Systém zpráv typu publikování/odběr vám umožňuje oddělit poskytovatele informací od spotřebitelů těchto informací. Odesílající aplikace a přijímající aplikace nemusí o sobě vědět nic o tom, které informace mají být odeslány a přijaty.

Před tím, než může aplikace IBM WebSphere MQ mezi dvěma body poslat zprávu do jiné aplikace, musí o této aplikaci vědět něco. Například potřebuje znát název fronty, do které se mají odeslat informace, a může také uvést název správce front.

IBM WebSphere MQ publish/subscribe odstraní potřebu vaší aplikace vědět cokoliv o cílové aplikaci. Všechny odesílající aplikace musí dělat, vloží zprávu IBM WebSphere MQ obsahující informace, které chce, a přiřadit jí téma, které označuje předmět informace, a umožní IBM WebSphere MQ zpracovat distribuci těchto informací. Podobně cílová aplikace nemusí vědět nic o zdroji informací, které obdrží.

Obrázek 3 na stránce 20 zobrazuje nejjednodušší systém publikování/odběr. K dispozici je jeden vydavatel, jeden správce front a jeden odběratel. Odběr se odešle z odběratele do správce front, z vydavatele se odešle publikace do správce front a poté je publikace předá správci front.



Obrázek 3. Konfigurace jednoduchého publikování/odběru

Typický systém publikování/odběru má více než jednoho vydavatele a více než jednoho odběratele a často více než jednoho správce front. Aplikace může být jak vydavatel, tak i odběratel.

## Přehled komponent publikování/odběru

Publikování/odběr je mechanismus, podle kterého mohou odběratelé přijímat informace ve formě zpráv od vydavatelů. Interakce mezi vydavatelem a odběrateli jsou řízeny správci front pomocí standardních prostředků produktu WebSphere MQ .

Typický systém publikování/odběru má více než jednoho vydavatele a více než jednoho odběratele a často více než jednoho správce front. Aplikace může být jak vydavatel, tak i odběratel.

Poskytovatel informací se nazývá *vydavatel*. Vydavatelé poskytují informace o předmětu, aniž by potřebovali vědět cokoli o aplikacích, které mají o tyto informace zájem. Vydavatelé generují tyto informace ve formě zpráv s názvem *publications* , které chtějí publikovat a definovat téma těchto zpráv.

Příjemce informací se nazývají *odběratel*. Odběratelé vytvářejí *odběry* popisující téma, o které se odběratel zajímá. Tento odběr určuje, které publikace jsou postoupeny odběrateli. Odběratelé mohou vytvářet více odběrů a mohou přijímat informace od mnoha vydavatelů.

Publikované informace jsou odeslány ve zprávě produktu WebSphere MQ a předmět informací je identifikován pomocí *tématu*. Vydavatel určuje téma při publikování informací a odběratel určuje témata, o kterých chce přijímat publikování. Odběratel je odeslán informace o pouze těch tématech, k nimž se přihlašuje.

Jedná se o existenci témat, která umožňují oddělit poskytovatele a spotřebitele informací v systému zpráv publikování/odběru tím, že odebere potřebu zahrnutí určitého místa určení do každé zprávy, jak je požadováno v systému zpráv typu point-to-point.

Interakce mezi vydavatelem a odběrateli jsou všechny řízeny správcem front. Správce front přijímá zprávy od vydavatelů a odběry od odběratelů (do rozsahu témat). Úloha správce front slouží ke směrování publikovaných zpráv na odběratele, kteří zaregistrovali zájem o dané téma zpráv.

Standardní prostředky produktu WebSphere MQ se používají k distribuci zpráv, takže aplikace mohou využívat všechny funkce, které jsou dostupné pro existující aplikace produktu WebSphere MQ . To znamená, že můžete použít trvalé zprávy, abyste získali once-only zajištěné doručení, a že vaše zprávy mohou být součástí transakční jednotky práce, abyste zajistili, že zprávy budou doručeny odběrateli pouze tehdy, jsou-li potvrzeny vydavatelem.

## Příklad konfigurace publikování/odběru pro jednu správce front

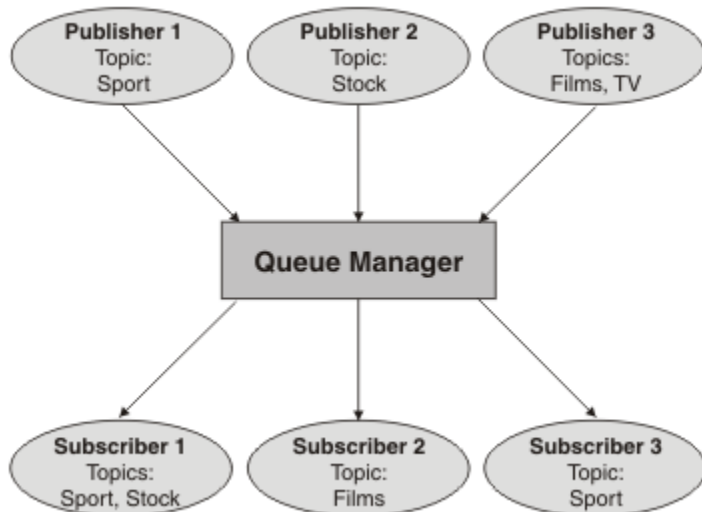
Obrázek 4 na stránce 21 ilustruje konfiguraci publikování/odběru základního jediného správce front. Příklad ukazuje konfiguraci služby news, kde jsou informace k dispozici od vydavatelů o několika tématech:

- Vydavatel 1 zveřejňuje informace o sportovních výsledcích pomocí tématu Sport
- Vydavatel 2 publikuje informace o cenách akcií za použití tématu Burzovní
- Vydavatel 3 zveřejňuje informace o filmových recenzích pomocí tématu Films, a o televizních filmech pomocí témat TV

Dva odběratelé zaregistrovali zájem o různá témata, takže správce front jim odešle informace, které se zajímají o:

- Odběratel 1 přijímá sportovní výsledky a ceny akcií
- Odběratel 2 obdrží filmové recenze
- Odběratel 3 přijímá sportovní výsledky

Žádný z účastníků nezaregistroval zájem o televizní výpisy, takže se nešíří.



Obrázek 4. Příklad publikování/odběru jednoho správce front

## Vydavatelé a publikování

V produktu WebSphere MQ publish/subscribe je vydavatel aplikací, která zpřístupňuje informace o určitém tématu správci front ve formě standardní zprávy produktu WebSphere MQ nazývané publikování. Vydavatel může publikovat informace o více než jednom tématu.

Vydavatelé používají příkazové slovo MQPUT k vložení zprávy do dříve otevřeného tématu, tato zpráva je publikace. Lokální správce front poté směřuje publikování na všechny odběratele, kteří mají odběry tématu publikování. Publikovanou zprávu může spotřebovat více než jeden odběratel.

Kromě rozdělení publikací na všechny lokální odběratele, kteří mají odpovídající odběry, může správce front také distribuovat publikování všem ostatním správcům front, kteří jsou k němu připojeni, buď přímo, nebo prostřednictvím sítě správců front, kteří mají odběratele k tomuto tématu.

V síti WebSphere MQ publish/subscribe může být vydavatelská aplikace také odběratelem.

### Publikování pod synchronizačním bodem

Vydavatelé mohou volat volání MQPUT nebo MQPUT1 v synchronizačním bodu, aby zahrnul všechny zprávy doručené odběratelům v pracovní jednotce. Je-li zadána volba MQPMO\_RETAIN nebo volby doručení tématu NPMSGDLV nebo PMSGDLV s hodnotami ALL nebo ALLDUR, správce front použije interní volání MQPUT nebo MQPUT1 v synchronizačním bodě v rámci rozsahu volání MQPUT vydavatele nebo volání MQPUT1 vydavatele.

### Informace o stavu a událostech

Publikace mohou být kategorizovány buď jako stavová publikace, jako např. aktuální cena akcie nebo publikování událostí, jako je například obchod s touto zásobami.

### Publikování stavu

*Státní publikace* obsahují informace o aktuálním stavu něčeho, jako je například cena akcie nebo aktuální skóre fotbalového utkání. Pokud se něco stane (například změni se cena akcie nebo dojde ke změně skóre), předchozí informace o stavu již není potřeba, protože je nahrazena novou informací.

Odběratel bude chtít při spuštění obdržet aktuální verzi informací o stavu a odesílat nové informace pokaždé, když se stav změni.

Pokud publikace obsahuje informace o stavu, je často publikována jako zachovaná publikace. Nový odběratel obvykle okamžitě chce informace o aktuálním stavu okamžitě; odběratel nechce čekat na událost, která způsobí opětovné publikování informací. Odběratelé automaticky obdrží zachované publikování tématu, pokud se přihlásí k odběru, pokud odběratel nepoužije volby MQSO\_PUBLICATIONS\_ON\_REQUEST nebo MQSO\_NEW\_PUBLICATIONS\_ONLY.

## **Publikování událostí**

*Publikování událostí* obsahují informace o jednotlivých událostech, k nimž dochází, jako je například obchod s některými akciemi nebo hodnocení konkrétního cíle. Každá událost je na ostatních událostech nezávislá.

Odběratel bude chtít přijímat informace o událostech, jak se stávají.

## **Zachovaná publikování**

Ve výchozím nastavení je po odeslání všem zainteresovaným odběratelům vyřazen. Vydavatel však může určit, že kopie publikace bude zachována, aby mohla být odeslána na budoucí odběratele, kteří se zajímají o dané téma.

Odstranění publikací poté, co byly odeslány všem zainteresovaným odběratelům, je vhodné pro informace o události, ale není vždy vhodná pro informace o stavu. Pokud zachováte zprávu, nové odběratele nemusí čekat, až budou informace znovu publikovány, dříve než obdrží počáteční informace o stavu. Například odběratel s odběrem na akciovou cenu by dostal aktuální cenu rovnou, aniž by čekal na změnu ceny akcií (a tedy i znovu zveřejnit).

Správce front může zachovat pouze jedno publikování pro každé téma, takže existující zachované publikování tématu je při doručení nového zachovaného publikování ve správci front odstraněno. Avšak odstranění existující publikace se nemusí vyskytnout synchronně s příchodem nové zachované publikace. Proto pokud je to možné, neodesílá více vydavatelů žádná publikování v libovolném tématu.

Odběratelé mohou určit, že nechtějí přijímat zachovaná publikování, pomocí volby odběru MQSO\_NEW\_PUBLICATIONS\_ONLY. Existující odběratelé mohou požádat o odeslání duplicitní kopie zachovaných publikování.

Existují okamžiky, kdy si možná nebudete chtít uchovat publikace, dokonce i pro informace o stavu:

- Pokud jsou všechny odběry tématu provedeny před provedením jakýchkoli publikování v daném tématu a neočekáváte nebo nepovolíte nové odběry, není třeba uchovávat žádné publikace, protože jsou doručeny kompletním množem odběratelů při prvním publikování těchto odběrů.
- Pokud k publikování dochází často, jako např. za sekundu, obdrží nový odběratel (nebo odběratel zotavující se z selhání) aktuální stav téměř okamžitě po jejich počátečním odběru, takže tyto publikace není třeba uchovávat.
- Jsou-li publikace velké, můžete pro každé téma uložit zachované publikování, které potřebuje značnou velikost úložného prostoru. V prostředí s více správci front jsou zachovaná publikování uložena všemi správci front v síti, které mají odpovídající odběr.

Při rozhodování o tom, zda mají být použity zachované publikace, zvažte možnost zotavení aplikací z odběru ze selhání. Pokud vydavatel nepoužívá zachovaná publikování, může být aplikace odběratele lokálně uložena do svého aktuálního stavu.

Chcete-li se ujistit, že je publikace zachována, použijte volbu vložení zprávy MQPMO\_RETAIN. Je-li tato volba použita a publikování nelze zadržet, zpráva se nepublikuje a volání selže s hodnotou MQRC\_PUT\_NOT\_RETAILED.

Je-li zpráva zachovaná publikování, je tato zpráva označena vlastností zprávy MQIsRetained . Perzistence zprávy je tak, jak byla, když byla původně publikována.

### **Publikace pod synchronizačním bodem**

V produktu IBM WebSphere MQ publish/subscribe může být synchronizační bod použit vydavatelem nebo interně správcem front.

Vydavatelé používají synchronizační bod, když vydají volání MQPUT/MQPUT1 s volbou MQPMO\_SYNCPOINT. Všechny zprávy doručené odběratelům se započítávají do maximálního počtu nepotvrzených zpráv v jednotce work.The Atribut správce front MAXUMSGS uvádí tento limit. Je-li dosaženo limitu, vydavatel obdrží kód příčiny 2024 (07E8) (RC2024): MQRC\_SYNCPOINT\_LIMIT\_REACHED .

Když vydavatel vydá volání MQPUT/MQPUT1 pomocí volby MQPMO\_NO\_SYNCPOINT s volbou MQPMO\_RETAIN nebo s volbami doručení tématu NPMMSGDLV/PMSGDLV s hodnotami ALL nebo ALLDUR, správce front použije vnitřní synchronizační body k zaručení toho, že jsou zprávy doručeny podle požadavku. Vydavatel může přijmout kód příčiny 2024 (07E8) (RC2024): MQRC\_SYNCPOINT\_LIMIT\_REACHED , je-li dosažen limit v rozsahu volání MQPUT/MQPUT1 vydavatele.

### **Odběratelé a odběry**

V produktu WebSphere MQ publish/subscribe je odběratel aplikací, který vyžaduje informace o specifickém tématu ze správce front v síti typu publikování/odběr. Odběratel může přijímat zprávy o stejných nebo různých tématech, a to od více než jednoho vydavatele.

Odběry mohou být vytvořeny ručně pomocí příkazu MQSC nebo aplikací. Tyto odběry jsou vydávány pro lokálního správce front a obsahují informace o publikacích, které chce odběratel přijmout:

- Téma, o které se odběratel zajímá; lze jej přeložit na více témat, jsou-li použity zástupné znaky.
- Volitelný výběrový řetězec, který má být použit na publikované zprávy.
- Manipulátor s frontou (označovanou jako *fronta odběratele*), na které mají být umístěny vybrané publikace, a volitelné CorrelId.

Lokální správce front ukládá informace o odběru a poté, co obdrží publikování, zkontroluje informace a určí, zda existuje odběr, který odpovídá tématu publikování a výběru řetězce. Pro každý odpovídající odběr správce front směřuje publikování do fronty odběratele odběratele. Informace, které správce front ukládá o odběrech, lze zobrazit pomocí příkazů služby DIS SUB a DIS SBSTATUS.

Odběr se odstraní pouze v případě, že dojde k jedné z následujících událostí:

- Odběratel se nepřihlašuje k odběru pomocí volání MQCLOSE (pokud byl odběr proveden nedurivě).
- Platnost odběru vyprší.
- Přihlášení je odstraněno administrátorem systému pomocí příkazu DELETE SUB.
- Aplikace odběratele se ukončí (pokud byl odběr proveden nedurivě).
- Správce front je zastaven nebo znovu spuštěn (pokud byl odběr proveden nedurivě).

Při získávání zpráv použijte příslušné volby na volání MQGET. Pokud vaše aplikace zpracovává pouze zprávy pro jeden odběr, měli byste použít `get-by-correlid`, jak je předvedeno v ukázkovém programu C `amqssbxa.c` a v nespravovaném odběrateli MQ. Hodnota **CorrelId** pro použití je vrácena z MQSUB v MQSD.Pole **SubCorrelId** .

### **Spravované fronty a publikování/odběr**

Při vytváření odběru můžete zvolit způsob použití spravovaných front. Pokud při vytváření odběru dojde k automatickému vytvoření fronty odběru, je fronta odběru vytvořena automaticky. Spravované fronty se tišují automaticky v souladu se stálostí odběru. Použití spravovaných front znamená, že se nemusíte starat o vytváření front pro příjem publikování a všechny nespoteřované publikování budou automaticky odebrány z front odběratele, je-li uzavřeno netrvalé připojení k odběru.

Pokud aplikace nemá potřebu používat určitou frontu jako její frontu odběratele, cíl pro publikování, které přijímá, může využívat *spravované odběry* pomocí volby odběru MQSO\_MANAGED. Pokud vytvoříte

spravovaný odběr, správce front vrátí obslužnou rutinu objektu pro odběratele pro frontu odběratele, kterou správce front vytvoří tam, kde budou přijaty publikování. Bude vrácen popisovač objektu fronty, který vám umožní procházet, získat nebo dotázat se na frontu (není možné vkládat nebo nastavovat atributy spravované fronty, pokud jste explicitně neposkytl přístup k dočasným dynamickým frontám).

Trvalost odběru určuje, zda je spravovaná fronta i nadále po přerušení připojení aplikace odběru ke správci front po přerušení.

Spravované odběry jsou obzvláště užitečné při použití s netrvalnými odběry, protože při ukončení připojení aplikace zůstanou nespoteřované zprávy ve frontě odběratele nadále zabrané ve správci front neomezeně dlouho. Pokud používáte spravovaný odběr, bude spravovaná fronta dočasnou dynamickou frontou a jako taková bude odstraněna spolu s libovolnými nespoteřovanými zprávami při přerušení připojení z následujících důvodů:

- Je použit příkaz MQCLOSE s MQCO\_REMOVE\_SUB a spravovaný objekt Hobj je uzavřen.
- dojde ke ztrátě připojení k aplikaci s použitím trvalého odběru (MQSO\_NON\_DURABLE).
- Odběr byl odebrán, protože jeho platnost vypršela a spravovaný objekt Hobj je uzavřen.

Spravované odběry lze také použít s trvalými odběry, ale je možné, že budete chtít nechat nespoteřované zprávy ve frontě odběratele, aby je bylo možné načíst při opětovném otevření připojení. Z tohoto důvodu jsou spravované fronty pro trvalé odběry ve formě trvalé dynamické fronty a zůstanou při přerušení připojení odebírající aplikace ke správci front.

Pokud chcete používat trvalou dynamickou spravovanou frontu, můžete nastavit vypršení platnosti, takže ačkoli fronta bude stále existovat i po přerušení spojení, nebude nadále existovat po neomezenou dobu.

Pokud odstraníte spravovanou frontu, obdržíte chybovou zprávu.

Spravované fronty, které jsou vytvořeny, jsou pojmenovány s čísly na konci (časová razítka) tak, aby byla každá jedinečná.

### **Trvalost odběru**

Odběry lze nakonfigurovat tak, aby byly trvalé nebo přechodné. Trvalost odběru určuje, co se stane s odběry při odpojování odebíraných aplikací od správce front.

### **Trvalé odběry**

Trvalé odběry existují i po zavření připojení odebírající aplikace ke správci front. Pokud je odběr trvalý, při odpojení odběratelské aplikace zůstává odběr na místě a může být použit odběratelskou aplikací, když znovu připojí požadavek na odběr znovu s použitím SubName, který byl vrácen při vytvoření odběru.

Při přihlášení k odběru je požadován název odběru (SubName). Názvy odběrů musí být v rámci správce front jedinečné, aby bylo možné jej použít k identifikaci odběru. Tento způsob identifikace je nezbytný při uvedení odběru, který chcete obnovit, pokud jste buď úmyslně zavřel popisovač do odběru (pomocí volby MQCO\_KEEP\_SUB), nebo jste byli odpojeni od správce front. Existující odběr můžete obnovit pomocí volání MQSUB s volbou MQSO\_RESUME. Názvy odběrů se zobrazí také v případě, že použijete příkaz DISPLAY SBSTATUS s hodnotou SUBTYPE ALL nebo ADMIN.

Pokud již aplikace nevyžaduje trvalý odběr, je možné ji odebrat pomocí volání funkce MQCLOSE s volbou MQCO\_REMOVE\_SUB, nebo ji lze odstranit ručně pomocí příkazu MQSC DELETE SUB.

Určuje, zda lze provádět trvalé odběry tématu s použitím atributu tématu produktu **DURSUB**.

Při návratu z volání MQSUB s použitím volby MQSO\_RESUME je vypršení platnosti odběru nastaveno na původní vypršení platnosti odběru a nikoli na zbývající dobu vypršení platnosti.

Správce front i nadále odesílá publikování, aby splnil trvalý odběr i v případě, že aplikace odběratele není připojena. To vede k sestavení zpráv ve frontě odběratele. Nejjednodušším způsobem, jak se tomuto problému vyhnout, je použít netrvalý odběr všude tam, kde je to vhodné. Pokud je však nutné používat trvalé odběry, lze se vyhnout sestavení zpráv, pokud se odběratel přihlásí k odběru pomocí volby Zachovaná publikování. Odběratel může poté řídit, kdy přijímá publikování, pomocí volání MQSUBRQ.



## Netrvalé odběry

Přechodné odběry existují pouze po dobu, kdy je otevřena připojení odebírající aplikace ke správci front. Tento odběr je odebrán, když se odběratelská aplikace odpojí od správce front, ať už úmyslně nebo kvůli ztrátě připojení. Po zavření připojení budou informace o odběru odebrány ze správce front a nebudou nadále zobrazeny, pokud se zobrazují odběry používající příkaz DISPLAY SBSTATUS. Žádné další zprávy nejsou vloženy do fronty odběratele.

Co se stane s nespotebnyými publikacemi ve frontě odběratele pro netrvalé odběry, je určena následujícím způsobem.

- Pokud odebírající aplikace používá spravované místo určení, budou všechny publikování, které nebyly spotřebovány, automaticky odebrány.
- Pokud odebírající aplikace poskytuje při přihlášení k odběru vlastní frontu odběratele, nespotebované zprávy se automaticky neodeberou. Je-li to vhodné, nese odpovědnost za to, že žádost je vhodná. Pokud je fronta sdílena více než jedním odběratelem nebo jinými aplikacemi typu point-to-point, nemusí být vhodné úplně vymazat frontu.

Správce front jej sice používá, i když není vyžadováno pro netrvalé odběry, pokud je zadán i název odběru. Názvy odběrů musí být v rámci správce front jedinečné, aby bylo možné jej použít k identifikaci odběru.

## Výběrové řetězce

*Řetězec výběru* je výraz, který se použije na publikování, aby se určilo, zda odpovídá odběru. Výběrové řetězce mohou obsahovat zástupné znaky.

Když se přihlásíte k odběru, kromě uvedení tématu můžete zadat řetězec výběru pro výběr publikací podle jejich vlastností zprávy.

## Témata

Téma je předmětem informací, které jsou publikovány ve zprávě publikování/odběru.

Zprávy v systému PPP se posílají na určitou cílovou adresu. Zprávy v systémech publikování/odběru založené na předmětu jsou odeslány odběratelům na základě předmětu, který popisuje obsah zprávy. V systémech založených na obsahu se zprávy odesílají odběratelům na základě obsahu samotné zprávy.

Systém publikování/odběru IBM WebSphere MQ je systém založený na předmětu a systému odběru. Vydavatel vytvoří zprávu a publikuje ji spolu s řetězcem tématu, který nejlépe odpovídá předmětu publikování. Chcete-li přijímat publikování, odběratel vytvoří odběr s použitím řetězce tématu shodujícího se na vzorek, který bude vybírat témata publikování. Správce front doručuje publikování odběratelům, kteří mají odběry, které odpovídají tématu publikování, a jsou autorizováni k přijetí těchto publikování. Článek, “Řetězce tématu” na stránce 26, popisuje syntaxi řetězců témat, které identifikují předmět publikace. Odběratelé také vytvářejí řetězce témat k výběru témat, která mají být zasílána. Řetězce témat, které odběratelé mohou vytvořit, mohou obsahovat dva alternativní schéma zástupných znaků pro shodu vzoru vůči řetězcům témat v příručkách. Porovnávání se vzory je popsáno v “Režimy zástupných znaků” na stránce 27.

V publikovat/subscribe-based publish/subscribe, vydavatelé nebo administrátoři jsou zodpovědní za klasifikaci předmětů do témat. Typicky jsou témata uspořádána hierarchicky, do stromu témat pomocí znaku ' / ' pro vytvoření podtémat v řetězci tématu. Příklady stromů témat viz “Stromy témat” na stránce 33. Témata jsou uzly ve stromu témat. Témata mohou být listové uzly bez dalších dílčích témat nebo zprostředkujících uzlů s dílčími tématy.

Paralelně s uspořádáním předmětů do hierarchického stromu témat můžete asociovat témata s objekty administrativních témat. Atributy přiřazujete k tématu, jako je například informace o tom, zda je téma rozděleno do klastru, a to tak, že jej přidružíte k objektu tématu administrace. Přidružení se provádí pojmenováním tématu pomocí atributu TOPICSTR objektu administrativního tématu. Pokud k tématu explicitně nepřidružíte objekt administrativního tématu, téma zdědí atributy nejbližšího předchůdce ve stromu témat, který *máte* přidružený k objektu administrativního tématu. Pokud jste nedefinovali žádná nadřazená témata vůbec, zdědí se z SYSTEM.BASE.TOPIC. Objekty administrativního tématu jsou popsány v tématu “Objekty administrativního tématu” na stránce 35.

**Poznámka:** I v případě, že dědíte všechny atributy tématu z SYSTEM.BASE.TOPIC, definujte kořenové téma pro svá témata, která přímo dědí z SYSTEM.BASE.TOPIC. Například v prostoru témat amerických států, USA/Alabama USA/Alaskaatd. USA je kořenové téma téma. Hlavním účelem kořenového tématu je vytvořit diskrétní, nepřekrývající se prostory témat, aby se zabránilo publikování shodujících se s chybnými odběry. To také znamená, že můžete změnit atributy vašeho kořenového tématu, aby se ovlivnilo celý prostor tématu. Můžete například nastavit název atributu **CLUSTER**.

Když se odkazujete na téma jako vydavatel nebo odběratel, máte možnost zadat řetězec tématu odkazující na objekt tématu nebo můžete provést obojí. V takovém případě bude zadaný řetězec tématu definovat dílčí téma objektu tématu. Správce front identifikuje téma připojením řetězce tématu k předponě řetězce tématu uvedeným v objektu tématu a vkládá mezi tyto dva řetězce témat další prvek ' / ', například *string/string string/object string*. “Kombinování řetězců témat” na stránce 31 popisuje toto dále. Výsledný řetězec tématu se používá k identifikaci tématu a k jeho přidružení k objektu administrativního tématu. Objekt administrativního tématu nemusí být nutně totožný s objektem tématu jako objekt tématu odpovídající hlavnímu tématu.

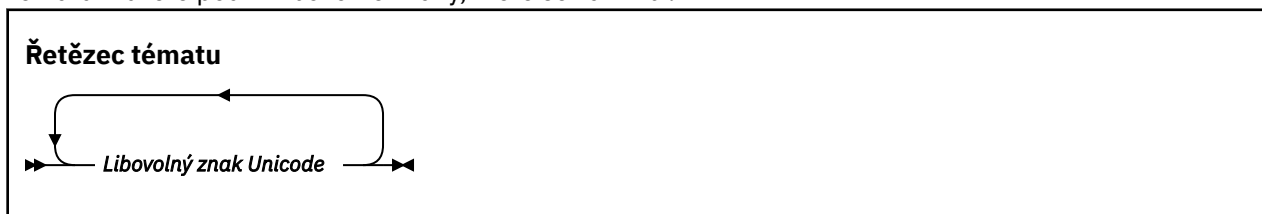
Při publikování/odběru založeného na obsahu definujete, které zprávy chcete přijímat, poskytnutím řetězců výběru, které prohledávají obsah každé zprávy. Produkt WebSphere MQ poskytuje zprostředkující formu publikování/odběru založeného na obsahu pomocí selektorů zpráv, které skenují vlastnosti zpráv, a ne úplný obsah zprávy, viz *Selektory*. Archetypní použití selektorů zpráv má být přihlášené k odběru tématu a poté kvalifikovat výběr pomocí číselné vlastnosti. Selektor vám umožňuje uvést, že se zajímáte o hodnoty pouze v určitém rozsahu; něco, co nemůžete provést pomocí zástupných znaků nebo zástupných znaků založených na tématu. Potřebujete-li filtrovat na základě celého obsahu zprávy, musíte použít produkt WebSphere Message Broker.

## Řetězce tématu

Informace o jmenovkách, které publikujete jako téma pomocí řetězce tématu. Přihlaste se k odběru skupin témat pomocí řetězců témat zástupných znaků založených na znacích nebo tématu.

## Témata

Řetězec tématu je znakový řetězec identifikující téma zprávy publikování/odběru. Při vytváření řetězce tématu můžete použít libovolné znaky, které se vám líbí.



Tři znaky mají speciální význam ve verzi 7 publish/subscribe. Jsou povoleny kdekoli v řetězci tématu, ale používají je s opatrností. Použití speciálních znaků je vysvětleno v části “Schéma zástupných znaků založených na tématu” na stránce 27.

### dopředné lomítko (/)

Oddělovač úrovně témat. Chcete-li strukturovat téma do stromu témat, použijte znak ' / ' .

Vyhnete se prázdným úrovním tématu, ' / / ', pokud můžete. Tyto odpovídají uzlům v hierarchii témat bez řetězce tématu. Vedoucí nebo koncový znak ' / ' v řetězci tématu odpovídá počátečnímu nebo koncovému prázdnému uzlu a je třeba se mu vyhnout.

### Znak křížku (#)

Používá se v kombinaci s ' / ' k vytvoření zástupného znaku více úrovní v odběrech. Dávejte pozor na '# ' sousedící s ' / ' v řetězcích témat použitých k pojmenování publikovaných témat. “Příklady řetězců témat” na stránce 27 zobrazuje citlivé použití '# ' .

Řetězce ' . . . /# / . . . ', '# / . . . ' a ' . . . /# ' mají speciální význam v řetězcích témat odběru. Řetězce se shodují se všemi tématy na jedné nebo více úrovních v hierarchii témat. Takže pokud jste vytvořili téma s jednou z těchto posloupností, nelze se k němu přihlásit, aniž byste se také přihlásili k odběru všech témat na více úrovních v hierarchii témat.

## Znaménko plus (+)

Používá se v kombinaci s '/' k vytvoření zástupného znaku single-level v odběrech. Dávejte pozor na '+' sousedící s '/' v řetězcích témat použitých k pojmenování publikovaných témat.

Řetězce '.../+/...', '+/...' a '.../+' mají speciální význam v řetězcích témat odběru. Řetězce se shodují se všemi tématy na jedné úrovni v hierarchii témat. Takže pokud jste vytvořili téma s jednou z těchto posloupností, nemůžete se přihlásit k odběru, aniž byste se také přihlásili k odběru všech témat na jedné úrovni v hierarchii témat.

## Příklady řetězců témat

```
IBM/Business Area#/Results
IBM/Diversity/%African American
```

### Režimy zástupných znaků

K odběru více témat se používají dva režimy zástupných znaků. Volba schématu je volba odběru.

### MQSO\_WILDCARD\_TOPIC

Chcete-li se přihlásit k odběru pomocí schématu zástupných znaků založeného na tématu, vyberte témata.

Toto je výchozí, pokud není explicitně vybráno žádné schéma zástupného znaku.

### MQSO\_WILDCARD\_CHAR

Chcete-li se přihlásit k odběru pomocí schématu zástupných znaků pro charakterizaci, vyberte témata.

Nastavte buď schéma zadáním parametru **wschema** v příkazu DEFINE SUB. Další informace viz [DEFINE SUB](#).

**Poznámka:** Odběry, které byly vytvořeny před produktem WebSphere MQ verze 7.0, vždy používají schéma zástupných znaků s použitím znaků.

## Příklady

```
IBM/+/Results
#/Results
IBM/Software/Results
IBM/*ware/Results
```

### Schéma zástupných znaků založené na tématu

Zástupné znaky založené na tématu umožňují odběratelům přihlásit se k odběru více než jednoho tématu současně.

Zástupné znaky založené na tématu jsou mocnou funkcí systému témat v publikaci WebSphere MQ publish/subscribe. Zástupné znaky více úrovní a zástupné znaky jedné úrovně lze použít pro odběry, nemohou ale být použity v rámci tématu vydavatelem zprávy.

Schéma zástupných znaků založené na tématu vám umožňuje vybrat publikace seskupené podle úrovně témat. Můžete zvolit *každou úroveň v hierarchii témat*, zda řetězec v odběru pro danou úroveň tématu se musí přesně shodovat s řetězcem v publikování, či nikoli. Například odběr vybere produkt IBM/+/Results všechna témata.

```
IBM/Software/Results
IBM/Services/Results
IBM/Hardware/Results
```

Existují dva typy zástupných znaků.

### Zástupný znak více úrovní

- Zástupný znak více úrovní se používá v předplatných. Při použití v publikaci se s ním zachází jako s literálem.

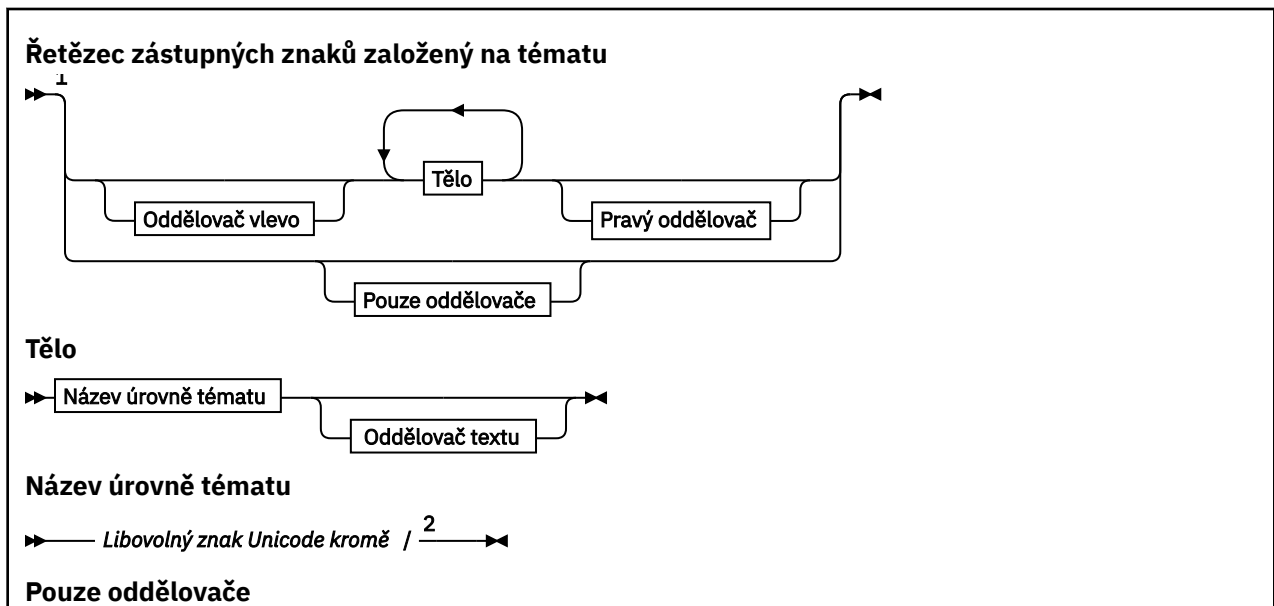
- Zástupný znak více úrovní '#' se používá ke shodě s libovolným počtem úrovní v rámci tématu. For example, using the example topic tree, if you subscribe to 'USA/Alaska/#', you receive messages on topics 'USA/Alaska' and 'USA/Alaska/Juneau'.
- Zástupný znak více úrovní může představovat nula nebo více úrovní. Proto 'USA/#' může také odpovídat singulární 'USA', kde '#' představuje nulové úrovně. Oddělovač úrovně témat v tomto kontextu postrádá smysl, protože nejsou žádné úrovně k oddělení.
- Zástupný znak více úrovní je platný pouze v případě, že je zadán samostatně nebo vedle znaku oddělovače úrovně tématu. Proto platí, že '#' a 'USA/#' jsou platná témata, kde se s znakem '#' zachází jako se zástupným znakem. Ačkoli však 'USA#' je také platným řetězcem tématu, znak '#' se nepovažuje za zástupný znak a nemá žádný speciální význam. Další informace viz [“Pokud zástupné znaky založené na tématu nejsou zástupné”](#) na stránce 30.

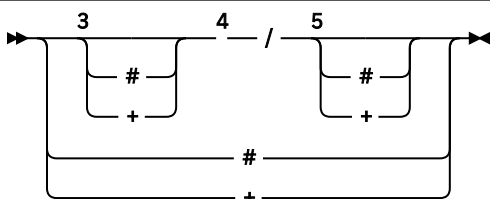
### Zástupný znak jedné úrovně

- Jeden zástupný znak se používá v odběrech. Při použití v publikaci se s ním zachází jako s literálem.
- Zástupný znak single-level '+' odpovídá jednomu, a pouze jedné úrovni tématu. Například, 'USA/+' odpovídá 'USA/Alabama', ale ne 'USA/Alabama/Auburn'. Protože zástupný znak single-level odpovídá pouze jedné úrovni, 'USA/+' se neshoduje s 'USA'.
- Zástupný znak jednotného místa lze použít na libovolné úrovni stromu témat a ve spojení s víceúrovňového zástupným znakem. Zástupný znak jednotného místa musí být zadán vedle oddělovače úrovně témat, s výjimkou případů, kdy je tento oddělovač zadán samostatně. Proto platí, že '+' a 'USA/+' jsou platná témata, kde se s znakem '+' zachází jako se zástupným znakem. Ačkoli však 'USA+' je také platným řetězcem tématu, znak '+' se nepovažuje za zástupný znak a nemá žádný speciální význam. Další informace viz [“Pokud zástupné znaky založené na tématu nejsou zástupné”](#) na stránce 30.

Syntaxe pro schéma zástupných znaků založené na tématu nemá žádné řídicí znaky. Zda jsou '#' a '+' považovány za zástupné znaky nebo ne, závisí na jejich kontextu. Další informace viz [“Pokud zástupné znaky založené na tématu nejsou zástupné”](#) na stránce 30.

**Poznámka:** Počátek a konec řetězce tématu je zpracováván speciálním způsobem. Using '\$' označuje konec řetězce, pak '\$#/...' je víceúrovňový zástupný znak a '\$#/...' je prázdný uzel v kořenovém adresáři, následovaný víceúrovňovým zástupným znakem.

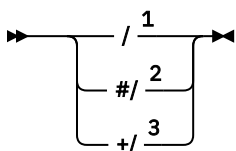




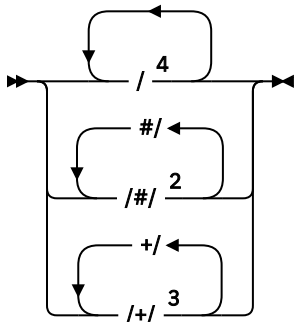
Poznámky:

- 1 Řetězec tématu s hodnotou Null nebo s nulovou délkou je neplatný.
- 2 Doporučuje se nepoužívat žádný z řetězců názvu produktu \*, ?, % pro kompatibilitu s použitím zástupných schémat založených na řetězci a schématech založených na tématu.
- 3 Tyto případy jsou ekvivalentní se vzorem *left delimiter*.
- 4 / bez zástupných znaků se shoduje s jedním prázdným tématem.
- 5 Tyto případy jsou ekvivalentní ke vzoru *right delimiter*.
- 6 Shoda se všemi tématy.
- 7 Shoda každé téma tam, kde je pouze jedna úroveň.

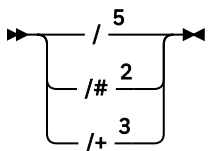
### Levý oddělovač



### Oddělovač textu



### Pravý oddělovač



Poznámky:

- 1 Řetězec tématu začíná prázdným tématem
- 2 Odpovídá nule nebo více úrovním. Vícenásobný řetězec shody na úrovni více úrovní má stejný účinek jako jeden řetězec s více shodnými řetězci.
- 3 Odpovídá přesně jedné úrovni.
- 4 // je prázdné téma-objekt tématu bez řetězce tématu.
- 5 Řetězec tématu končí prázdným tématem

## Pokud zástupné znaky založené na tématu nejsou zástupné

Zástupné znaky '+' a '#' nemají žádný speciální význam, jsou-li směřovány s ostatními znaky (včetně sebe) na úrovni tématu.

To znamená, že témata, která obsahují '+' nebo '#' společně s ostatními znaky na úrovni témat, mohou být publikována.

Vezměme si například následující dvě témata:

1. level0/level1/+/level4/#
2. level0/level1/#+/level4/level#

V prvním příkladu jsou znaky '+' a '#' považovány za zástupné znaky, a proto nejsou platné v řetězci tématu, který má být publikován, ale je platný v odběru.

Ve druhém příkladu nejsou znaky '+' a '#' považovány za zástupné znaky, a proto může být řetězec tématu publikován i odebírán.

### Příklady

```
IBM/+/Results
#/Results
IBM/Software/Results
```

#### Schéma zástupných znaků založených na znacích

Schéma zástupného znaku na základě znaků vám umožňuje vybrat témata založená na tradiční shodě znaků.

Můžete vybrat všechna témata na více úrovních v hierarchii témat pomocí řetězce '\*'. Použití produktu '\*' ve schématu zástupných znaků s použitím znaků je ekvivalentní použití řetězce zástupného znaku '#' založeného na tématu.

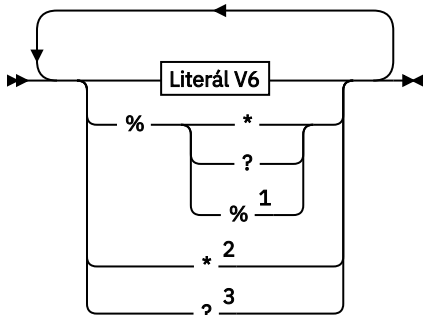
'x\*/y' je ekvivalentní příkazu 'x#/y' v rámci schématu založeném na tématu a vybírá všechna témata v hierarchii témat mezi úrovněmi 'x' a 'y', kde 'x' a 'y' jsou názvy témat, které nejsou v sadě úrovní vrácených zástupným znakem.

'+/ ' v rámci schématu založeného na tématu nemá v rámci schématu na základě znaků žádný přesný ekvivalent. 'IBM\*/Results' by také vybral 'IBM/Patents/Software/Results'. Pouze v případě, že je sada názvů témat na každé úrovni hierarchie jedinečná, můžete vždy vytvářet dotazy se dvěma schématy, které vedou identické shody.

Obecně platí, že '\* a '?' v systému založeném na popisu nemají žádné ekvivalenty v rámci schématu založeném na tématu. Schéma založené na tématu neprovádí částečné shody s použitím zástupných znaků. Odběr zástupného znaku založený na znacích 'IBM\*/ware/Results' neobsahuje žádný ekvivalent na základě témat.

**Poznámka:** Shody používající zástupné znaky zástupných znaků jsou pomalejší než shody s použitím odběrů založených na tématu.

#### Řetězec zástupných znaků založených na znacích



## Literál V6

►► *Jakýkoliv znak Unicode kromě \*;? a%* ◄◄

Poznámky:

- <sup>1</sup> Znamená to "Escape the following character", takže se s ním zachází jako s literálem. Za '%' musí následovat buď '\*', '?' nebo '%'. Viz "Příklady řetězců témat" na stránce 27.
- <sup>2</sup> Znamená "Shoda s nulou nebo více znaky" v odběru.
- <sup>3</sup> Znamená "Shoda přesně jednoho znaku" v odběru.

## Příklady

```
IBM/*/Results  
IBM/*ware/Results
```

## Kombinování řetězců témat

Při vytváření odběrů nebo otevírání témat, abyste pro ně mohli publikovat zprávy, může být řetězec tématu vytvořen kombinací dvou samostatných řetězců dílčích témat nebo "dílčích témat". Jeden dílčí téma je poskytováno aplikací nebo administrativním příkazem jako řetězec tématu a druhým je řetězec tématu přidružený k objektu tématu. Jako řetězec tématu můžete použít buď dílčí téma jako řetězec tématu, nebo je zkombinovat a vytvořit nový název tématu.

Pokud například definujete odběr pomocí příkazu MQSC **DEFINE SUB**, může příkaz provést buď **TOPICSTR** (řetězec tématu), nebo **TOPICOBJ** (objekt tématu) jako atribut, nebo oboje současně. Je-li zadán pouze příznak **TOPICOBJ**, bude řetězec tématu asociovaný s daným objektem tématu použit jako řetězec tématu. Je-li zadán pouze příznak **TOPICSTR**, bude použit jako řetězec tématu. Jsou-li zadány oba parametry, jsou zřetězeny tak, že tvoří jeden řetězec tématu ve tvaru **TOPICOBJ/TOPICSTR**, kde je řetězec tématu **TOPICOBJ** konfigurován vždy jako první a obě části řetězce jsou vždy odděleny znakem "/" .

Podobně se v programu MQI vytvoří úplný název tématu produktem MQOPEN. Skládá se ze dvou polí používaných ve voláních publikování/odběru MQI, v uvedeném pořadí:

1. Atribut **TOPICSTR** objektu tématu, pojmenovaný v poli **ObjectName** .
2. Parametr **ObjectString** definující dílčí téma poskytované aplikací.

Výsledný řetězec tématu se vrátí v parametru **ResObjectString** .

Tato pole se považují za přítomná, pokud první znak každého pole není prázdný znak nebo znak null a délka pole je větší než nula. Je-li přítomno pouze jedno z těchto polí, použije se nezměněno jako název tématu. Pokud pole nemá hodnotu, volání selže s kódem příčiny MQRC\_UNKNOWN\_OBJECT\_NAME nebo MQRC\_TOPIC\_STRING\_ERROR , je-li úplný název tématu neplatný.

Jsou-li přítomna obě pole, je znak "/" vložen mezi dva prvky výsledného kombinovaného názvu tématu.

Tabulka 2 na stránce 31 zobrazuje příklady zřetězení řetězce tématu:

TOPICSTR objektu tématu	Řetězec tématu poskytnutý aplikací nebo příkazem DEFINE SUB	Úplný název tématu	Komentář
Fotbal/Scores	' '	Fotbal/Scores	TOPICSTR objektu tématu se používá samostatně.
' '	Fotbal/Scores	Fotbal/Scores	Parametr ObjectString/ TOPICSTR se používá samostatně.

Tabulka 2. Příklady zřetězení řetězce tématu (pokračování)

TOPICSTR objektu tématu	Řetězec tématu poskytnutý aplikací nebo příkazem DEFINE SUB	Úplný název tématu	Komentář
Fotbal	Skóre	Fotbal/Scores	Znak "/" je přidán do bodu zřetězení.
Fotbal	/Skóre	Fotbal//skóre	Mezi dvěma řetězci se vytváří 'prázdný uzel'. Tato hodnota se liší od položky "Fotbal/Skóre".
/Fotbal	Skóre	/Fotbal/Scores	Téma začíná znakem 'empty node'. Tato hodnota se liší od položky "Fotbal/Skóre".

Znak "/" je považován za speciální znak a poskytuje strukturu úplnému názvu tématu v produktu "Stromy témat" na stránce 33. Znak "/" nesmí být použit z žádného jiného důvodu, protože struktura stromu témat je ovlivněna. Téma "/Football" není stejné jako téma "Football".

**Poznámka:** Použijete-li při vytváření odběru objektu tématu, bude hodnota řetězce tématu objektu tématu v rámci odběru definována v době definování. Jakákoli další změna objektu tématu nemá vliv na řetězec tématu, na který je odběr definován.

## Zástupné znaky v řetězcích témat

Následující zástupné znaky jsou speciální znaky:

- znaménko plus (+)
- znak čísla (#)
- hvězdička (\*)
- otazník (?)

Zástupné znaky mají při použití u odběru speciální význam. Tyto znaky se při použití jinde nepovažují za neplatné, ale musíte zajistit, abyste porozuměli tomu, jak jsou tyto znaky používány, a při publikování nebo definování objektů tématu můžete raději nepoužívat tyto znaky ve svých řetězcích témat.

Pokud publikujete na řetězec tématu s # nebo + smíchaným s ostatními znaky (včetně samotných) v rámci úrovně tématu, může být řetězec tématu přihlášen k odběru buď pomocí zástupných schémat.

Pokud publikujete na řetězec tématu s # nebo + jako jediný znak mezi dvěma znaky / , řetězec tématu nemůže být odebírán explicitně aplikací pomocí schématu zástupného znaku MQSO\_WILDCARD\_TOPIC. Tato situace vede k tomu, že aplikace bude dostávat více publikací, než se očekávalo.

V řetězci tématu definovaného objektu tématu byste neměli používat zástupný znak. Pokud tak učiníte, je tento znak považován za literálový znak, je-li objekt používán vydavatelem, a jako zástupný znak při použití odběru. To může vést k zmatku.

## Příklad úseku kódu

Tento úsek kódu extrahovaný z ukázkového programu [Příklad 2: Vydavatel na téma s proměnnou](#) kombinuje objekt tématu s řetězcem tématu s proměnnou:

```
MQOD      td = {MQOD_DEFAULT}; /* Object Descriptor          */
td.ObjectType = MQOT_TOPIC; /* Object is a topic    */
td.Version = MQOD_VERSION_4; /* Descriptor needs to be V4 */
strcpy(td.ObjectName, topicName, MQ_TOPIC_NAME_LENGTH);
td.ObjectString.VSPtr = topicString;
td.ObjectString.VSLength = (MQLONG)strlen(topicString);
```



```
td.ResObjectString.VSPtr = resTopicStr;
td.ResObjectString.VSBufSize = sizeof(resTopicStr)-1;
MQOPEN(Hconn, &td, MQOO_OUTPUT | MQOO_FAIL_IF QUIESCING, &Hobj, &CompCode, &Reason);
```

## Stromy témat

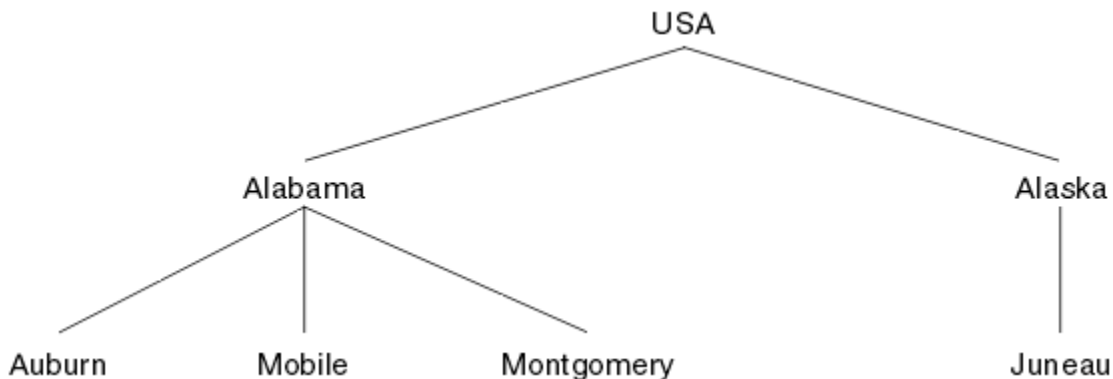
Každé téma, které definujete, je prvkem, neboli uzlem, stromu témat. Strom témat může být buď prázdný, aby mohl začínat nebo obsahovat témata, která byla definována dříve pomocí příkazů MQSC nebo PCF. Nové téma můžete definovat buď pomocí příkazů k vytvoření tématu, nebo zadáním tématu pro první publikování nebo odběr.

I když můžete použít libovolný řetězec znaků k definování řetězce tématu, je vhodné zvolit řetězec tématu, který se vejde do hierarchické stromové struktury. Promyšlený návrh struktur témat a stromů témat vám může pomoci s následujícími operacemi:

- Přihlášení k odběru více témat.
- Vytváření zásad zabezpečení.

Ačkoli můžete vytvořit strom témat jako fixní, lineární strukturu, je lepší sestavit strom témat v hierarchické struktuře s jedním nebo více kořenovými tématy. Další informace o plánování zabezpečení a tématech naleznete v tématu [Zabezpečení publikování a odběru](#).

Příklad [Obrázek 5 na stránce 33](#) ukazuje příklad stromu témat s jedním kořenovým tématem.



Obrázek 5. Příklad stromu témat

Každý znakový řetězec na obrázku představuje uzel ve stromu témat. Úplný řetězec tématu se vytváří agregací uzlů z jedné nebo více úrovní ve stromu témat. Úrovně jsou odděleny znakem "/". Formát plně specifikovaného řetězce témat je: "root/level2/level3".

Platná témata ve stromu témat, která jsou uvedena v části [Obrázek 5 na stránce 33](#), jsou:

```
'USA'
"USA/Alabama"
"USA/Aljaška"
"USA/Alabama/Auburn"
"USA/Alabama/Mobile"
"USA/Alabama/Montgomery"
"USA/Aleska/Juneau"
```

Když navrhujete řetězce témat a stromy témat, nezapomeňte, že správce front není interpretován nebo se pokouší odvodit význam samotného řetězce tématu. Jednoduše používá řetězec tématu k odeslání vybraných zpráv odběratelům daného tématu.

Na konstrukci a obsah stromu témat se vztahují následující zásady:

- Počet úrovní ve stromu témat není omezen počtem úrovní.
- Délka názvu ve stromu témat není nijak omezena délkou názvu.
- Může existovat libovolný počet "kořenových" uzlů; to znamená libovolný počet stromů témat.

### *Snížení počtu nežádoucích témat ve stromu témat*

Výkon systému publikování/odběru se zlepšil snížením počtu nežádoucích témat ve stromu témat. Co je nežádoucí téma a jak je chcete odstranit?

Můžete vytvořit velký počet témat bez nepříznivého ovlivnění výkonu. Nicméně některé způsoby použití výsledků publikování/odběru mají za následek neustálé rozbalování stromů témat. Výjimečně velký počet témat se vytvoří jednou a nikdy nebude použit znovu. Rostoucí počet témat se může stát problémem s výkonem.

Jak se můžete vyhnout návrhům, které vedou k velkému a rostoucímu počtu nechtěných témat? Co můžete udělat, chcete-li pomoci správci front odebrat nežádoucí témata ze stromu témat?

Správce front rozpozná nežádoucí téma, protože bylo nepoužívané po dobu 30 minut. Správce front odebere nepoužívaná témata ze stromu témat za vás. Doba trvání 30 minut může být změněna změnou atributu správce front **TREELIFE**. Můžete pomoci správci front odebrat nežádoucí témata tím, že se ujistíte, že se dané téma objevuje ve správci front, který má být použit. Část [“Co je nepoužité téma?”](#) na stránce 34 vysvětluje, o jaké nepoužívané téma se jedná.

Programátor, návrh jakékoli aplikace a zejména návrh dlouho běžící aplikace, se domnívá, že jeho využití prostředků: kolik prostředků tento program vyžaduje, jsou zde nějaké nevázané požadavky a všechny úniky prostředků? Témata jsou prostředek, který používají programy pro publikování/odběr. Zbarvujte použití témat stejně jako ostatní prostředky, které program používá.

## **Co je nepoužité téma?**

Před definováním toho, co je nepoužité téma, jaké přesně se počítá jako téma?

Je-li řetězec tématu (například USA/Alabama/Auburn) převeden na určité téma, bude téma přidáno do stromu témat. V případě potřeby jsou ve stromu vytvořeny další uzly témat a příslušná témata, která jsou vytvořena ve stromu. Řetězec tématu USA/Alabama/Auburn se převede na strom se třemi tématy.

- USA
- USA/Alabama
- USA/Alabama/Auburn

Chcete-li zobrazit všechna témata ve stromu témat, použijte příkaz **runmqsc DISPLAY TPSTATUS ('#' ) TYPE(TOPIC)** .

Nepoužité téma ve stromu témat má následující vlastnosti.

### **Není přidružen k objektu tématu**

Objekt administrativního tématu má řetězec tématu, který jej přidružuje k tématu. Definujete-li objekt tématu Alabama , je-li téma USA/Alabama, které má být přidruženo k dispozici, neexistuje, bude téma vytvořeno z řetězce tématu. Pokud téma existuje, objekt tématu spolu s tématem jsou asociovány společně s použitím řetězce tématu.

### **Neobsahuje zachované publikování**

Téma s zachovaným výsledkem publikování má za následek, že vydavatel vloží zprávu do tématu s volbou **MQPMO\_RETAIN** .

Příkaz **runmqsc DISPLAY TPSTATUS ('USA/Alabama ') RETAINED** se používá ke kontrole, zda má USA/Alabama zachované publikování. Odezva je YES nebo NO.

Chcete-li odebrat zachované publikování z produktu USA/Alabama , použijte příkaz **runmqsc CLEAR TOPICSTR ('USA/Alabama ') CLTRTYPE (RETAINED)** .

### **Nemá žádná podřízená témata**

USA/Alabama/Auburn je téma s žádnými podřízenými tématy. USA/Alabama/Auburn je téma přímého podřízeného prvku USA/Alabama.

Zobrazit přímé podřízené prvky USA/Alabama s příkazem **runmqsc DISPLAY TPSTATUS ('USA/Alabama/+ ')** .

## K uzlu nejsou žádní aktivní vydavatelé

Aktivní vydavatel pro uzel je aplikace, která má otevřené téma pro výstup.

Např. aplikace otevře objekt tématu s názvem **Alabama** s volbami otevření MQOO\_OUTPUT.

Chcete-li zobrazit aktivní vydavatele pro USA/Alabama a všechny jeho podřízené položky, použijte příkaz **runmqsc DISPLAY TPSTATUS('USA/Alabama/#') TYPE(PUB) ACTCONN**.

## Neexistují žádní aktivní odběratelé uzlu

Aktivní odběratel může být buď trvalý odběr, nebo aplikace, která zaregistrovala odběr k tématu s produktem MQSUB, a nikoli k jeho zavření.

Chcete-li zobrazit aktivní odběry pro USA/Alabama, použijte příkaz **runmqsc DISPLAY TPSTATUS('USA/Alabama') TYPE(SUB) ACTCONN**.

Chcete-li zobrazit aktivní odběry pro USA/Alabama a všechny její podřízené prvky, použijte příkaz **runmqsc DISPLAY TPSTATUS('USA/Alabama/#') TYPE(SUB) ACTCONN**.

## Omezení počtu témat ve stromu témat

V souhrnu je řada způsobů, jak snížit počet témat ve stromu témat.

### Upravit TREELIFE

Nepoužité téma má standardně dobu trvání 30 minut. Životnost nepoužitého tématu můžete provést menší.

Například příkaz **runmqsc , ALTER QMGR TREELIFE(900)**, zkracuje dobu životnosti nepoužitého tématu z 30 minut na 15 minut.

### Výjimečně restartujte správce front.

Při restartování správce front je strom témat znovu inicializován z objektů tématu, uzlů s zachovanými publikováními a trvalých odběrů. Témata, která byla vytvořena operací vydavatele a programů odběratele, jsou eliminována.

Příkaz **runmqsc DISPLAY TPSTATUS('#') TYPE(TOPIC)** pravidelně slouží k zobrazení seznamu všech témat a kontrole, zda se počet zvětšoval.

Jako poslední možnost, pokud byl růst v nechtěných tématech příčinou problémů s výkonem v minulosti, restartujte správce front.

## Objekty administrativního tématu

Pomocí objektu administrativního tématu můžete jednotlivým tématům přiřazovat specifické, nevýchozí atributy.

Obrázek 6 na stránce 35 ukazuje, jak lze vizualizovat téma vysoké úrovně Sport rozdělené do samostatných témat pokrývajících různé sporty jako strom témat:



Obrázek 6. Vizualizace stromu témat

Obrázek 7 na stránce 36 ukazuje, jak lze strom témat rozdělit dále, aby oddělil různé typy informací o každém sportu:



Obrázek 7. Rozšířený strom témat

Chcete-li vytvořit strom témat ilustrovaný, není třeba definovat žádné objekty administrativního tématu. Každý z uzlů v tomto stromu je definován řetězcem tématu vytvořeným v rámci operace publikování nebo odběru. Každé téma ve stromu dědí své atributy od svého nadřazeného. Atributy jsou zděděny z nadřazeného objektu tématu, protože při výchozím nastavení jsou všechny atributy nastaveny na hodnotu ASPARENT. V tomto příkladu má každé téma stejné atributy jako téma Sport . Téma Sport nemá žádný objekt administrativního tématu a dědí jeho atributy z `SYSTEM.BASE.TOPIC`.

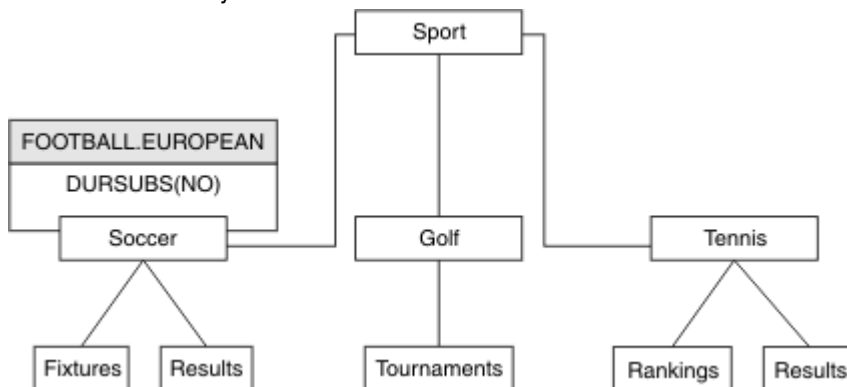
Všimněte si, že není dobrým zvykem dávat oprávnění pro uživatele, kteří nejsou mqm, v kořenovém uzlu stromu témat, což je `SYSTEM.BASE.TOPIC`, protože oprávnění jsou děděna, ale nemohou být omezena. Tím, že udělavám orgánům na této úrovni, dáváte úřadům celý strom. Oprávnění by mělo být uděleno na nižší úrovni témat v hierarchii.

Administrativní objekty témat lze použít k definování specifických atributů pro konkrétní uzly ve stromu témat. V následujícím příkladu je definován objekt administrativního tématu k nastavení vlastnosti trvalé odběry `DURSUB` na fotbalové téma na hodnotu `NO`:

```

DEFINE TOPIC(FOOTBALL.EUROPEAN)
TOPICSTR('Sport/Soccer')
DURSUB(NO)
DESCR('Administrative topic object to disallow durable subscriptions')
  
```

Strom témat lze nyní vizualizovat takto:



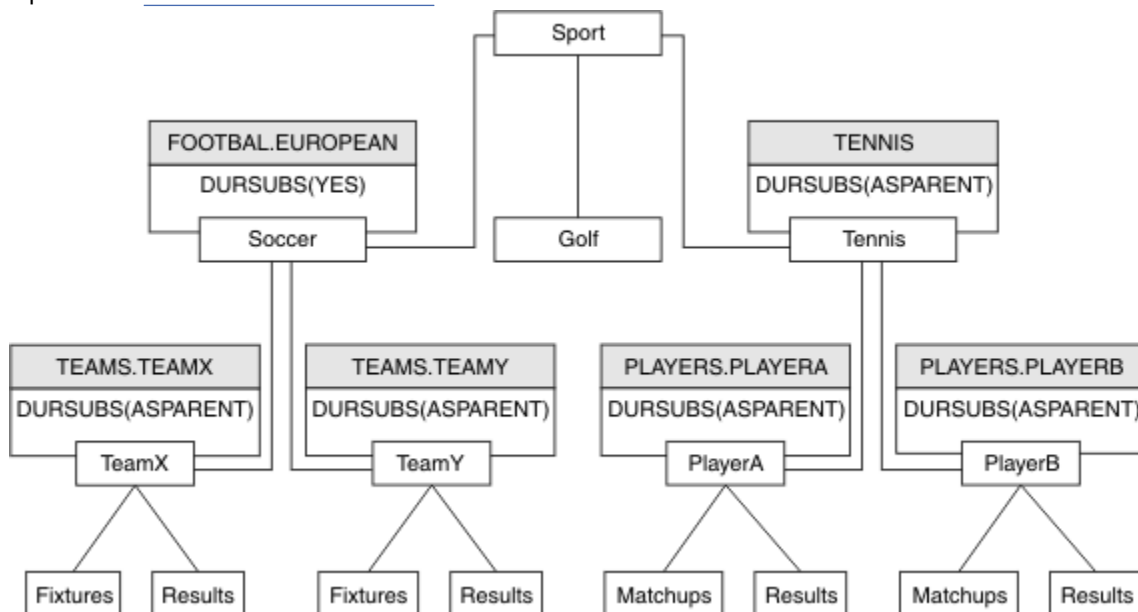
Obrázek 8. Vizualizace objektu administrativního tématu přidruženého k tématu Sport/Soccer

Všechny aplikace, které jsou přihlášeny k odběru témat pod Soccer ve stromu, stále mohou používat řetězce témat, které byly použity před přidáním objektu administrativního tématu. Nyní však může být aplikace zapsána k odběru s použitím názvu objektu `FOOTBALL.EUROPEAN`, namísto řetězce `/Sport/Soccer`. Chcete-li se například přihlásit k odběru `/Sport/Soccer/Results`, může aplikace zadat `MQSD`. `ObjectName` jako `FOOTBALL.EUROPEAN` a `MQSD`. `ObjectString` jako `Results`.

Pomocí této funkce můžete skrýt část stromu témat od vývojářů aplikací. Definujte objekt administrativních témat v konkrétním uzlu ve stromu témat a vývojáři aplikací pak mohou definovat vlastní témata jako podřazené prvky uzlu. Vývojáři musí vědět o nadřazeném tématu, ale ne o žádném jiném uzlu v nadřazeném stromu.

## Zdědění atributů

Pokud má strom témat mnoho objektů administrativních témat, každý objekt tématu správy standardně dědí své atributy od nejbližšího nadřazeného administrativního tématu. Předchozí příklad byl rozšířen v produktu [Obrázek 9 na stránce 37](#):



Obrázek 9. Strom témat s několika objekty administrativního tématu

Pokud například použijete dědičnost k poskytnutí všech podřízených témat /Sport/Soccer, vlastnosti, které odběry jsou netrvalé. Změňte atribut DURSUB z FOOTBALL.EUROPEAN na NO.

Tento atribut lze nastavit pomocí následujícího příkazu:

```
ALTER TOPIC(FOOTBALL.EUROPEAN) DURSUB(NO)
```

Všechny objekty administrativních témat podřízených témat produktu Sport/Soccer mají vlastnost DURSUB nastavenou na výchozí hodnotu ASPARENT. Po změně hodnoty vlastnosti DURSUB u FOOTBALL.EUROPEAN na NO podřízená témata Sport/Soccer dědí hodnotu vlastnosti DURSUB NO. Všechna podřízená témata Sport/Tennis dědí hodnotu od objektu DURSUB z objektu SYSTEM.BASE.TOPIC. SYSTEM.BASE.TOPIC má hodnotu YES.

Pokus o vytvoření trvalého odběru pro téma Sport/Soccer/TeamX/Results se nyní nezdaří. Pokus o vytvoření trvalého odběru pro produkt Sport/Tennis/PlayerB/Results by však byl úspěšný.

## Řízení použití zástupného znaku s vlastností WILDCARD

Pomocí vlastnosti MQSC Topic WILDCARD nebo ekvivalentních vlastností PCF Topic WildcardOperation můžete řídit doručování příruček aplikacím, které používají řetězce názvů témat zástupných znaků. Vlastnost WILDCARD může mít jednu ze dvou možných hodnot:

### WILDCARD

Chování odběrů používajících zástupné znaky s ohledem na toto téma.

#### PASSTHRU

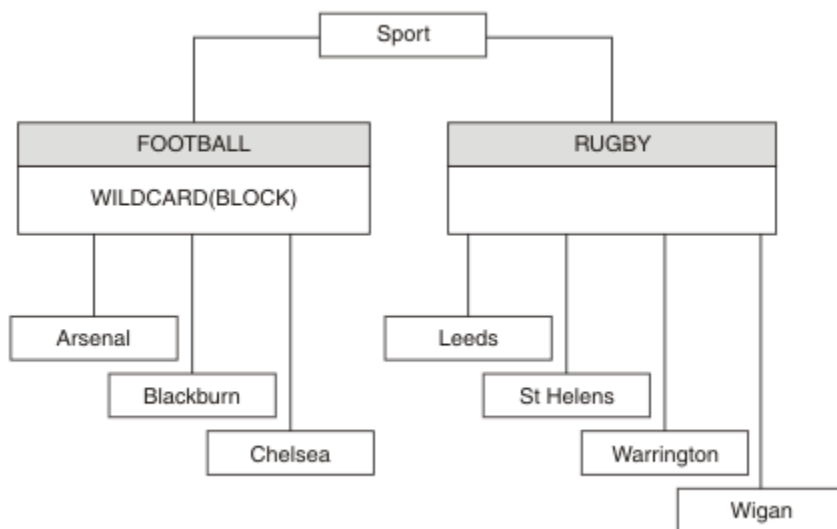
U odběrů registrovaných pro téma, které používá zástupné znaky a které je méně specifické než řetězec tématu v tomto objektu tématu, jsou poskytnuty publikace k tomuto tématu a k řetězcům tématu, které jsou specifičtější než toto téma.

#### BLOCK

U odběrů registrovaných pro téma, které používá zástupné znaky a které je méně specifické než řetězec tématu v tomto objektu tématu, nejsou poskytnuty publikace k tomuto tématu ani k řetězcům tématu, které jsou specifičtější než toto téma.

Hodnota tohoto atributu se použije při definici odběrů. Když tento atribut změníte, sada témat pokrytých existujícími odběry nebude touto změnou ovlivněna. Tento scénář platí i v případě, že se změnila topologie, tj. když byly objekty tématu vytvořeny nebo odstraněny. Sada témat odpovídajících odběrům, které byly vytvořeny po této změně atributu WILDCARD, se vytvoří s použitím této nové, upravené topologie. Pokud chcete vynutit opětovné vyhodnocení odpovídající sady témat pro existující odběry, musíte restartovat správce front.

V příkladu, “Příklad: Vytvoření klastru pro publikování/odběr produktu Sport” na stránce 42, můžete postupovat podle kroků k vytvoření stromové struktury témat, která je zobrazena v části Obrázek 10 na stránce 38.



Obrázek 10. Strom témat, který používá vlastnost WILDCARD , BLOCK .

Odběratel používající řetězec tématu s zástupnými znaky # přijímá všechny publikace k tématu Sport a podstromu Sport /Rugby . Odběratel neobdrží žádné publikace do podstromu Sport/Football , protože hodnota vlastnosti WILDCARD u tématu Sport/Football je BLOCK.

Výchozí nastavení je PASSTHRU . Hodnotu vlastnosti ZÁSTUPNÝ ZNAK PASSTHRU můžete nastavit na uzly ve stromu Sport . Pokud uzly nemají hodnotu vlastnosti WILDCARD BLOCK, nastavení PASSTHRU nezmění chování pozorované odběratelem na uzlech ve stromu Sports .

V tomto příkladu vytvořte odběry a zjistěte, jak nastavení zástupných znaků ovlivňuje doručené publikace, viz Obrázek 14 na stránce 43. Spusťte publikační příkaz v produktu Obrázek 17 na stránce 44 a vytvořte některé publikace.

pub QMA

Obrázek 11. Publikovat na QMA

Výsledky jsou zobrazeny v Tabulka 3 na stránce 38. Všimněte si, jak nastavení hodnoty vlastnosti WILDCARD BLOCK brání odběrům se zástupnými znaky z příjmu publikací na témata v rámci rozsahu zástupného znaku.

Tabulka 3. Publikace přijaté v systému QMA			
Předplatně	Řetězec tématu	Přijaté publikace	Poznámky
SPORTS	Sports/#	Sports Sports/Rugby Sports/Rugby/Leeds	Všechny publikace ve fotbalovém podstromu blokováné uživatelem WILDCARD (BLOCK) v systému Sports/Football

Tabulka 3. Publikace přijaté v systému QMA (pokračování)

Předplatník	Řetězec tématu	Přijaté publikace	Poznámky
SARSENAL	Sports/#/Arsenal	-	WILDCARD (BLOCK) v Sports/Football zabraňuje odběru zástupného znaku na Arsenal
SLEEDS	Sports/#/Leeds	Sports/Rugby/Leeds	Předvolba WILDCARD na Sports/Rugby nezabrání odběru zástupného znaku na Leeds.

#### Poznámka:

Předpokládejme, že odběr má zástupný znak, který odpovídá objektu tématu s hodnotou vlastnosti WILDCARD BLOCK. Má-li odběr také řetězec tématu napravo od odpovídajícího zástupného znaku, odběr nikdy neobdrží publikování. Sada publikací, které nejsou blokovány, jsou publikace k tématům, která jsou nadřazenými prvky blokováného zástupného znaku. Publikování do témat, která jsou podřízenými prvky tématu s hodnotou vlastnosti produktu BLOCK, jsou blokovány zástupnými znaky. Proto řetězce témat odběru, které obsahují téma napravo od zástupného znaku, nikdy nepřijímají žádné publikace, které by se shodovaly.

Nastavení hodnoty vlastnosti WILDCARD na hodnotu BLOCK neznámá, že se nemůžete přihlásit k odběru pomocí řetězce tématu, který obsahuje zástupné znaky. Takové předplatné je normální. Odběr má explicitní téma, které odpovídá danému tématu s objektem tématu, který má hodnotu vlastnosti WILDCARD BLOCK. Používá zástupné znaky pro témata, která jsou nadřazenými nebo podřízenými prvky tématu s hodnotou vlastnosti WILDCARD BLOCK. V příkladu v produktu Obrázek 10 na stránce 38 může odběr, jako je Sports/Football/#, přijímat publikování.

#### Zástupné znaky a témata klastru

Definice témat klastru jsou šířeny do všech správců front v klastru. Odběr tématu klastru v jednom správci front v klastru má za následek vytvoření proxy odběrů ve správci front. Proxy odběr je vytvořen ve všech ostatních správci front v klastru. Odběry pomocí řetězců témat obsahujících zástupné znaky, kombinované s tématy klastru, mohou být obtížné předpovědět chování. Chování je vysvětleno v následujícím příkladu.

V klastru nastavenými pro tento příklad, “Příklad: Vytvoření klastru pro publikování/odběr produktu Sport” na stránce 42, má QMB stejnou sadu odběrů jako QMA, ale QMB nepřijal žádné publikace poté, co vydavatel publikován na QMA, viz Obrázek 11 na stránce 38. Ačkoli témata Sports/Football a Sports/Rugby jsou témata klastru, odběry definované v souboru fullsubs.tst se neodkazují na téma klastru. Z produktu QMB do produktu QMA nejsou šířeny žádné odběry proxy. Bez odběrů proxy jsou do produktu QMB předávány žádné publikace QMA.

Některé odběry, jako např. Sports/#/Leeds, se mohou v tomto případě odkazovat na téma klastru Sports/Rugby. Odběr produktu Sports/#/Leeds je ve skutečnosti interpretováno jako objekt tématu SYSTEM.BASE.TOPIC.

Pravidlo pro vyřešení objektu tématu, na který se odkazuje odběr, jako je například Sports/#/Leeds, je následující. Ořízněte řetězec tématu na první zástupný znak. Skenování bylo ponecháno přes řetězec tématu, který hledá první téma, které má přidružený objekt administrativního tématu. Objekt tématu může určovat název klastru, nebo definovat lokální objekt tématu. V příkladu, Sports/#/Leeds, řetězec tématu po oseknutí je Sports, který nemá žádný objekt tématu, a tak se Sports/#/Leeds dědí od SYSTEM.BASE.TOPIC, což je lokální objekt tématu.

Chcete-li zjistit, jak může přihlášení k odběru klastrovaných témat změnit způsob, jakým šíření zástupných znaků funguje, spusťte dávkový skript upsubs.bat. Skript vymaže fronty odběru a přidá odběry témat klastru do adresáře fullsubs.tst. Znovu spusťte soubor puba.bat a vytvořte dávku publikací; viz Obrázek 11 na stránce 38.

Produkt Tabulka 4 na stránce 40 zobrazuje výsledek přidání dvou nových odběrů do stejného správce front, ve kterém byly publikovány publikace. Výsledkem je podle očekávání, že nové odběry obdrží jedno



publikování a počty publikování přijatých ostatními odběry budou nezměněny. Dojde k neočekávaným výsledkům na druhém správcí front klastru, viz [Tabulka 5](#) na stránce 40.

<i>Tabulka 4. Publikace přijaté v systému QMA</i>			
<b>Předplatně</b>	<b>Řetězec tématu</b>	<b>Přijaté publikace</b>	<b>Poznámky</b>
SPORTS	Sports/#	Sports Sports/Rugby Sports/Rugby/Leeds	Všechny publikace ve fotbalovém podstromu blokováné uživatelem WILDCARD (BLOCK) v systému Sports/Football
SARSENAL	Sports/#/Arsenal	-	WILDCARD (BLOCK) v Sports/Football zabraňuje odběru zástupného znaku na Arsenal
SLEEDS	Sports/#/Leeds	Sports/Rugby/Leeds	Předvolba WILDCARD na Sports/Rugby nezabrání odběru zástupného znaku na Leeds.
FARSENAL	Sports/Football/Arsenal	Sports/Football/Arsenal	Produkt Arsenal obdrží publikování, protože odběr nemá zástupný znak.
FLEEDS	Sports/Rugby/Leeds	Sports/Rugby/Leeds	Leeds obdrží publikování v každém případě.

Produkt [Tabulka 5](#) na stránce 40 zobrazuje výsledky přidání dvou nových odběrů v produktu QMB a publikování v produktu QMA. Připomeňme si, že produkt QMB nepřijal žádná publikování bez těchto dvou nových odběrů. Jak bylo očekáváno, tyto dva nové odběry přijímají publikace, protože Sports/FootBall a Sports/Rugby jsou obě témata klastru. QMB postoupil proxy odběry pro Sports/Football/Arsenal a Sports/Rugby/Leeds do QMA, které následně odeslaly publikace do QMB.

Neočekávaný výsledek je takový, že se dva odběry Sports/# a Sports/#/Leeds, které dříve neobdržely žádné publikace, nyní přijímají publikace. Důvodem je to, že publikace Sports/Football/Arsenal a Sports/Rugby/Leeds předané produktu QMB pro ostatní odběry jsou nyní k dispozici pro všechny odběratele připojené k produktu QMB. V důsledku toho se odběry lokálních témat Sports/# a Sports/#/Leeds přijímají v publikaci Sports/Rugby/Leeds. Produkt Sports/#/Arsenal nadále neobdrží publikování, protože sport/fotbal má nastavenou hodnotu vlastnosti WILDCARD nastavenou na hodnotu BLOCK.

<i>Tabulka 5. Publikace přijaté v systému QMB</i>			
<b>Předplatně</b>	<b>Řetězec tématu</b>	<b>Přijaté publikace</b>	<b>Poznámky</b>
SPORTS	Sports/#	Sports/Rugby/Leeds	Všechny publikace ve fotbalovém podstromu blokováné produktem WILDCARD (BLOCK) v systému Sports/Football
SARSENAL	Sports/#/Arsenal	-	WILDCARD (BLOCK) v Sports/Football zabraňuje odběru zástupného znaku na Arsenal
SLEEDS	Sports/#/Leeds	Sports/Rugby/Leeds	Výchozí hodnota WILDCARD na Sports/Rugby nezabrání odběru zástupných znaků v systému Leeds.
FARSENAL	Sports/Football/Arsenal	Sports/Football/Arsenal	Produkt Arsenal obdrží publikování, protože odběr nemá zástupný znak.



Tabulka 5. Publikace přijaté v systému QMB (pokračování)

Předplatník	Řetězec tématu	Přijaté publikace	Poznámky
FLEEDS	Sports/Rugby/Leeds	Sports/Rugby/Leeds	Leeds obdrží publikování v každém případě.

Ve většině aplikací je nežádoucí pro jeden odběr ovlivnit chování jiného odběru. Jedno důležité použití vlastnosti WILDCARD s hodnotou BLOCK znamená, že se odběry ke stejnému řetězci tématu, které obsahují zástupné znaky, budou chovat jednotně. Údaj o tom, zda je odběr ve stejném správcí front jako vydavatel nebo jiný, výsledky odběru jsou stejné.

## Zástupné znaky a proudy

Proudy produktu WebSphere MQ verze 6 jsou mapovány na témata prostřednictvím produktu WebSphere MQ verze 7; viz "Proudy a témata" na stránce 44 . Ve výchozím mapování, které je provedeno produktem **strmqbrk** ve verzi 7, by všechna témata v proudu Sports byla mapována na téma Sports. Všechna témata v proudu Business budou mapována na téma Business.

Odběr v produktu WebSphere MQ verze 6 až \* v proudu produktu Sports přijímá všechny publikace ve stromu Sports a ve stromu Business nejsou k dispozici žádné publikace. Stejný odběr ve verzi 7 by přijímal všechny publikace ve stromu Sports a ve všech publikacích ve stromu Business . K zablokování tohoto chování, když jsou proudy migrovány do verze 7, produkt **strmqbrk** nastaví vlastnost WILDCARD . Nastaví ji na hodnotu BLOCK pro každé z témat nejvyšší úrovně, které jsou migrovány z proudu. Vlastnost WILDCARD produktu Sports a Business je nastavena na hodnotu BLOCK podle převodu z proudů verze 6 s názvem Sports a Business.

Pro novou aplikaci napsanou na rozhraní API pro publikování/odběr je výsledkem, že odběr z produktu \* neobdrží žádné publikace. Chcete-li přijmout všechny sportovní publikace, musíte se přihlásit k odběru produktu Sports/\*nebo produktu Sports/# a podobně jako publikace Business .

Chování existující aplikace publikování/odběru ve frontě se při migraci zprostředkovatele publikování/odběru do produktu WebSphere MQ verze 7 nezmění. Vlastnost **StreamName** v příkazech **Publish**, **Register Publisher**nebo **Subscriber** je mapována na název tématu, na který byl proud migrován.

## Zástupné znaky a body odběru

WebSphere body odběrů zprostředkovatele zpráv jsou mapovány na témata pomocí produktu WebSphere MQ verze 7; viz "Body odběru a témata" na stránce 46. Ve výchozím mapování, které je provedeno produktem **migmqbrk** ve verzi 7, by všechna témata v bodu odběru Sports byla mapována na téma Sports. Všechna témata v bodu odběru Business by byla mapována na téma Business.

Odběr produktu WebSphere Message Broker verze 6 na \* v bodu odběru Sports přijímá všechny publikace ve stromu Sports a ve stromu Business nejsou žádné publikace. Stejný odběr ve verzi 7 by přijímal všechny publikace ve stromu Sports a ve všech publikacích ve stromu Business . Chcete-li blokovat toto chování, při migraci bodů odběru na verzi 7 nastaví produkt **migmqbrk** vlastnost WILDCARD . Nastaví ji na hodnotu BLOCK pro každé z témat nejvyšší úrovně, které jsou migrovány z bodu odběru. Vlastnost WILDCARD produktu Sports a Business je nastavena na hodnotu BLOCK převodem z bodů odběru produktu WebSphere Message Broker s názvem Sports a Business .

U nové aplikace napsané pro rozhraní API pro publikování/odběr je výsledkem migrace skutečnost, že odběr produktu \* přijímá žádné publikace. Chcete-li přijmout všechny sportovní publikace, musíte se přihlásit k odběru produktu Sports/\*nebo produktu Sports/# a podobně jako publikace Business .

Chování existující aplikace publikování/odběru ve frontě se při migraci zprostředkovatele publikování/odběru do produktu WebSphere MQ verze 7 nezmění. Vlastnost **SubPoint** v příkazech **Publish**, **Register Publisher**nebo **Subscriber** je mapována na název tématu, na které byl odběr migrován.

## Příklad: Vytvoření klastru pro publikování/odběr produktu Sport

Kroky následující po vytvoření klastru CL1se čtyřmi správci front: dvě úplná úložiště, CL1A a CL1B a dvě dílčí úložiště, QMA a QMB. Úplná úložiště se používají k zadržení pouze definic klastru. QMA je označen jako hostitel tématu klastru. Trvalé odběry jsou definovány na serveru QMA i v produktu QMB.

**Poznámka:** Příklad je kódován pro systém Windows. Chcete-li nakonfigurovat a otestovat tento příklad na jiných platformách, musíte soubor `Create qmgrs.bat` a `create pub.bat` nakonfigurovat a otestovat.

1. Vytvořte skriptové soubory.
  - a. [Vytvoření topics.tst](#)
  - b. [Vytvořit wildsubs.tst](#)
  - c. [Vytvořit fullsubs.tst](#)
  - d. [Vytvořit qmgrs.bat](#)
  - e. [create pub.bat](#)
2. Chcete-li vytvořit konfiguraci, spusťte příkaz `Create qmgrs.bat` .

```
qmgrs
```

Vytvořte témata v produktu [Obrázek 10](#) na stránce 38. Skript na obrázku 5 vytvoří témata klastru `Sports/Football` a `Sports/Rugby`.

**Poznámka:** Volba `REPLACE` nenahrazuje vlastnosti typu `TOPICSTR` v rámci tématu. `TOPICSTR` je vlastnost, která se používá v příkladu k testování různých stromů témat. Chcete-li změnit témata, odstraňte nejprve téma.

```
DELETE TOPIC ('Sports')
DELETE TOPIC ('Football')
DELETE TOPIC ('Arsenal')
DELETE TOPIC ('Blackburn')
DELETE TOPIC ('Chelsea')
DELETE TOPIC ('Rugby')
DELETE TOPIC ('Leeds')
DELETE TOPIC ('Wigan')
DELETE TOPIC ('Warrington')
DELETE TOPIC ('St. Helens')

DEFINE TOPIC ('Sports') TOPICSTR('Sports')
DEFINE TOPIC ('Football') TOPICSTR('Sports/Football') CLUSTER(CL1) WILDCARD(BLOCK)
DEFINE TOPIC ('Arsenal') TOPICSTR('Sports/Football/Arsenal')
DEFINE TOPIC ('Blackburn') TOPICSTR('Sports/Football/Blackburn')
DEFINE TOPIC ('Chelsea') TOPICSTR('Sports/Football/Chelsea')
DEFINE TOPIC ('Rugby') TOPICSTR('Sports/Rugby') CLUSTER(CL1)
DEFINE TOPIC ('Leeds') TOPICSTR('Sports/Rugby/Leeds')
DEFINE TOPIC ('Wigan') TOPICSTR('Sports/Rugby/Wigan')
DEFINE TOPIC ('Warrington') TOPICSTR('Sports/Rugby/Warrington')
DEFINE TOPIC ('St. Helens') TOPICSTR('Sports/Rugby/St. Helens')
```

*Obrázek 12. Odstraňte a vytvořte témata: topics.tst*

**Poznámka:** Odstraňte témata, protože produkt `REPLACE` nebude nahrazovat řetězce témat.

Vytvoření odběrů se zástupnými znaky. Zástupné znaky odpovídají tématům s objekty témat v produktu [Obrázek 10](#) na stránce 38. Vytvořte frontu pro každý odběr. Fronty jsou vymazány a odběry odstraněny, když je skript spuštěn nebo znovu spuštěn.

**Poznámka:** Volba `REPLACE` nenahrazuje vlastnosti `TOPICOBJ` nebo `TOPICSTR` odběru. `TOPICOBJ` nebo `TOPICSTR` jsou vlastnosti, které jsou užitečné v příkladu pro testování různých odběrů. Chcete-li je změnit, nejprve odstraňte odběr.

```

DEFINE QLOCAL(QSPORTS) REPLACE
DEFINE QLOCAL(QSARSENAL) REPLACE
DEFINE QLOCAL(QSLEEDS) REPLACE
CLEAR QLOCAL(QSPORTS)
CLEAR QLOCAL(QSARSENAL)
CLEAR QLOCAL(QSLEEDS)

DELETE SUB (SPORTS)
DELETE SUB (SARSENAL)
DELETE SUB (SLEEDS)
DEFINE SUB (SPORTS) TOPICSTR('Sports/#') DEST(QSPORTS)
DEFINE SUB (SARSENAL) TOPICSTR('Sports+/Arsenal') DEST(QSARSENAL)
DEFINE SUB (SLEEDS) TOPICSTR('Sports+/Leeds') DEST(QSLEEDS)

```

Obrázek 13. Vytvoření zástupných znaků pro zástupný znak: wildsubs.tst

Vytvořte odběry, které odkazují na objekty tématu klastru.

**Poznámka:**

Oddělovač, /, se automaticky vkládá mezi řetězec tématu, na který odkazuje TOPICOBJ, a řetězec tématu definovaný parametrem TOPICSTR.

Definice DEFINE SUB(FARSENAL) TOPICSTR('Sports/Football/Arsenal') DEST(QFARSENAL) vytváří stejný odběr. TOPICOBJ se používá jako rychlý způsob, jak odkazovat na řetězec tématu, který jste již definovali. Když se odběr vytvoří, již se nebude odkazovat na objekt tématu.

```

DEFINE QLOCAL(QFARSENAL) REPLACE
DEFINE QLOCAL(QRLEEDS) REPLACE
CLEAR QLOCAL(QFARSENAL)
CLEAR QLOCAL(QRLEEDS)

DELETE SUB (FARSENAL)
DELETE SUB (RLEEDS)
DEFINE SUB (FARSENAL) TOPICOBJ('Football') TOPICSTR('Arsenal') DEST(QFARSENAL)
DEFINE SUB (RLEEDS) TOPICOBJ('Rugby') TOPICSTR('Leeds') DEST(QRLEEDS)

```

Obrázek 14. Odstraňte a vytvořte odběry: fullsubs.tst

Vytvořte klastr se dvěma úložišti. Vytvořte dvě dílčí úložiště pro publikování a odběr. Znovu spusťte skript k odstranění všeho a začněte znovu. Skript také vytvoří hierarchii témat a počáteční zástupné znaky odběrů.

**Poznámka:**

Na ostatních platformách napište podobný skript nebo zadejte všechny příkazy. Pomocí skriptu lze rychle odstranit vše a začít znovu se stejnou konfigurací.

```

@echo off
set port.CL1B=1421
set port.CL1A=1420
for %%A in (CL1A CL1B QMA QMB) do call :createQM %%A
call :configureQM CL1A CL1B %port.CL1B% full
call :configureQM CL1B CL1A %port.CL1A% full
for %%A in (QMA QMB) do call :configureQM %%A CL1A %port.CL1A% partial
for %%A in (topics.tst wildsubs.tst) do runmqsc QMA < %%A
for %%A in (wildsubs.tst) do runmqsc QMB < %%A
goto:eof

:createQM
echo Configure Queue manager %1
endmqm -p %1
for %%B in (dlt crt str) do %%Bmqm %1
goto:eof

:configureQM
if %1==CL1A set p=1420
if %1==CL1B set p=1421
if %1==QMA set p=1422
if %1==QMB set p=1423
echo configure %1 on port %p% connected to repository %2 on port %3 as %4 repository
echo DEFINE LISTENER(LST%1) TRPTYPE(TCP) PORT(%p%) CONTROL(QMGR) REPLACE | runmqsc %1
echo START LISTENER(LST%1) | runmqsc %1
if full==%4 echo ALTER QMGR REPOS(CL1) DEADQ(SYSTEM.DEAD.LETTER.QUEUE) | runmqsc %1
echo DEFINE CHANNEL(TO.%2) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('LOCALHOST(%3)') CLUSTER(CL1)
REPLACE | runmqsc %1
echo DEFINE CHANNEL(TO.%1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('LOCALHOST(%p%)')
CLUSTER(CL1) REPLACE | runmqsc %1
goto:eof

```

Obrázek 15. Vytvoření správců front: qmgrs.bat

Aktualizujte konfiguraci přidáním odběrů do témat klastru.

```

@echo off
for %%A in (QMA QMB) do runmqsc %%A < wildsubs.tst
for %%A in (QMA QMB) do runmqsc %%A < upsubs.tst

```

Obrázek 16. Aktualizovat odběry: upsubs.bat

Spuštěním příkazu pub.bat se správcem front jako parametrem publikujete zprávy obsahující řetězec tématu publikování. Produkt Pub.bat používá vzorový program **amqspub**.

```

@echo off
@rem Provide queue manager name as a parameter
set S=Sports
set S=6 Sports/Football Sports/Football/Arsenal
set S=6 Sports/Rugby Sports/Rugby/Leeds
for %%B in (6) do echo %%B | amqspub %%B %1

```

Obrázek 17. Publikovat: pub.bat

## **Proudy a témata**

Publikování/odběr ve frontě má koncept proudu publikování, který neexistuje v integrovaném modelu publiku/odběru. Ve frontě publikovat/odebírat proudy poskytují způsob, jak oddělit tok informací pro různá témata. V produktu IBM WebSphere MQ Version 6.0 je proud implementován jako fronta, definovaná na každém zprostředkovateli, který podporuje proud. Každá fronta má stejný název (název daného proudu). Od produktu IBM WebSphere MQ Version 7.0 je proud implementován jako téma nejvyšší úrovně, které lze administrativně namapovat na jiný identifikátor tématu.

Výchozí proud SYSTEM.BROKER.DEFAULT.STREAM je nastaven automaticky pro všechny zprostředkovatele a správce front v síti a žádná další konfigurace není vyžadována pro použití výchozího proudu. Myslete na výchozí proud jako nepojmenovaný výchozí prostor tématu. Témata, která byla publikována do výchozího proudu, jsou okamžitě k dispozici všem připojeným zprostředkovatelům produktu Version 6.0 a všem správcům front od Version 7.0 s povoleným publikováním/odběrem ve frontě. Pojmenované proudy jsou jako samostatné pojmenované prostory témat. Pojmenovaný proud musí být definován na každém zprostředkovateli, kde se používá.

Při definování tématu je toto téma k dispozici pro zprostředkovatele publikování/odběru produktu Version 6.0 a pro vydavatele a odběratele spuštěné na novější verzi produktu IBM WebSphere MQbez speciální konfigurace.

Jsou-li vydavatelé a odběratelé v různých správcích front, potom jsou po připojení zprostředkovatelů ve stejné hierarchii zprostředkovatele, není vyžadována žádná další konfigurace pro publikování a odběry mezi nimi. Stejná interoperabilita funguje i v obráceném pořadí.

## Pojmenované proudy

Návrhář řešení, který pracuje s programovacím modelem publikování/odběru ve frontě, může rozhodnout o umístění všech sportovních publikací do pojmenovaného proudu nazvaného Sport. V produktu Version 6.0 se proud často replikuje automaticky na jiné zprostředkovatele, kteří používají modelovou frontu SYSTEM.BROKER.MODEL.STREAM. Aby však byl proud dostupný správci front spuštěnému v systému Version 7.0 ve frontě s povoleným publikováním/odběrem ve frontě, musí být proud přidán ručně.

Pokud migrujete správce front z produktu Version 6.0, spuštěním příkazu **strmqbrk** migruje Version 6.0 proudy s názvem proudu do témat. Proud Sport je mapován na téma Sport. Tento parametr nelze použít pro z/OS.

Aplikace typu publikování/odběr zařazené do fronty, které se přihlásí k odběru Soccer/Results v proudu Sport, se bez změny nemění. Integrované aplikace typu publikování/odběr, které se přihlašují k odběru tématu Sport pomocí produktu MQSUBa dodávají řetězec tématu Soccer/Results, obdrží také stejné publikace.

Je-li téma Soccer/Result vytvořeno produktem **strmqbrk**, je definováno jako podřízený prvek tématu Sports řetězcem tématu Sport. Odběr produktu Soccer/Results je realizován jako odběr produktu Sport/Soccer/Results, a tak jsou publikace do proudu produktu Sport mapovány na různé místo v prostoru témat na publikace do jiného proudu, například Business.

Existují scénáře, pro které není automatická migrace provedená produktem **strmqbrk** odpověď, a je třeba ručně přidat proudy. Úloha přidání proudu je popsána v tématu [Přidání proudu](#). Je možné, že budete muset ručně přidat proudy ze tří důvodů.

1. Pokračujete v údržbě aplikací publikování/odběru u správců front verze 6, které spolupracují s nově napsanými aplikacemi publikování/odběru spuštěnými v pozdějších správcích front.
2. Pokračujete v vytváření aplikací publikování/odběru ve frontě spuštěných v pozdějších správcích front verze, nikoli migrace aplikací do rozhraní modulu MQI publikování/odběru.
3. Výchozí mapování proudů na témata vede k "kolizi" v prostoru témat a publikace v proudu mají stejný řetězec tématu jako publikace odjinud.

## Oprávnění

Ve výchozím nastavení je v kořenovém adresáři stromu témat více objektů témat: SYSTEM.BASE.TOPIC, SYSTEM.BROKER.DEFAULT.STREAMa SYSTEM.BROKER.DEFAULT.SUBPOINT. Oprávnění (například pro publikování nebo odběr) jsou určována autoritami na serveru SYSTEM.BASE.TOPIC; všechny oprávnění na serveru SYSTEM.BROKER.DEFAULT.STREAM nebo SYSTEM.BROKER.DEFAULT.SUBPOINT se ignorují. Pokud je některý z SYSTEM.BROKER.DEFAULT.STREAM nebo SYSTEM.BROKER.DEFAULT.SUBPOINT odstraněn a znovu vytvořen s neprázdným řetězcem tématu, oprávnění definovaná na těchto objektech se používají stejným způsobem jako normální objekt tématu.

## Mapování mezi proudy a tématy

Proud publikování/odběru ve frontě je napodoben v produktu Version 7.0 tím, že vytváří frontu a dává jí stejný název jako proud. Někdy se fronta nazývá fronta proudu, protože taková je, jak se objevuje ve frontě aplikací typu publikování/odběr. Fronta je identifikována pro stroj publikování/odběru přidáním do speciálního seznamu názvů nazvaného SYSTEM.QPUBSUB.QUEUE.NAMELIST. Do seznamu názvů můžete přidat tolik proudů, kolik jich potřebujete, přidáním dalších speciálních front do seznamu názvů. Nakonec je třeba přidat témata se stejnými názvy jako proudy a stejné řetězce témat jako název proudu, takže můžete publikovat a odebírat témata.

Avšak za výjimečných okolností můžete udělit témata, která odpovídají proudům, všechny řetězce témat, které zvolíte při definování témat. Účelem řetězce tématu je poskytnout tématu jedinečný název v prostoru tématu. Typicky název proudu slouží tomuto účelu dokonale. Někdy se může název proudu a existující název tématu kolidovat. Chcete-li problém vyřešit, můžete zvolit jiný řetězec tématu pro téma přidružené k proudu. Vyberte libovolný řetězec tématu a ujistěte se, že je jedinečný.

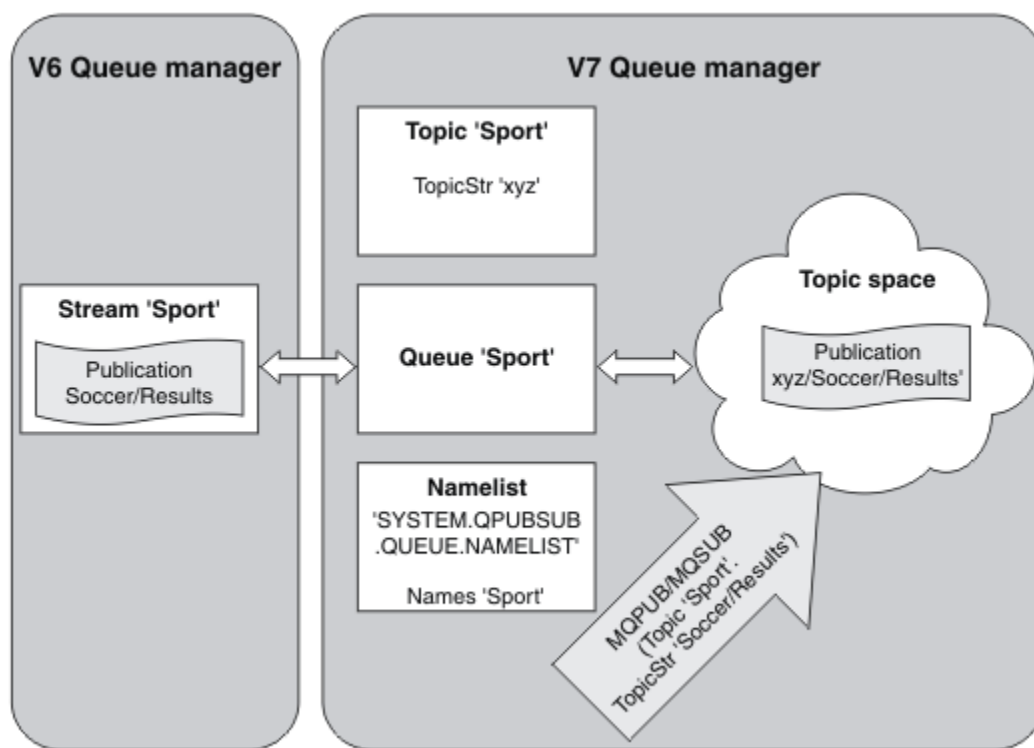
Řetězec tématu, který je definován v definici tématu, je uveden jako předpona k řetězci tématu poskytovaným vydavateli a odběrateli pomocí volání modulu MQOPEN nebo MQSUB MQI. Aplikace odkazující na témata používající objekty témat nejsou ovlivněny volbou předpony řetězce témat-a proto můžete zvolit libovolný řetězec tématu, který uchovává publikování jedinečné v prostoru tématu.

Přemapování různých proudů na různá témata se spoléhá na předpony použité pro řetězce témat, které jsou jedinečné, aby se oddělují jedna sada témat zcela od jiného. Musíte definovat konvenci pojmenování univerzálních témat, která bude přísně dodržována, aby mapování fungovalo. Pokud v produktu Version 7.0kolidované řetězce tématu kolidují, můžete použít proudy k oddělení prostorů témat. Počínaje verzí Version 7.0 používáte k přemapování řetězce tématu na jiné místo v prostoru tématu mechanismus předběžné opravy.

**Poznámka:** Odstraní-li proud, odstraňte nejprve všechny odběry z proudu. Tato akce je nejdůležitější, pokud některý z odběrů pochází od jiných zprostředkovatelů v hierarchii zprostředkovatele.

### Příklad

V produktu [Obrázek 18](#) na stránce 46 má téma 'Sport' řetězec tématu 'xyz', který má za následek, že publikace pocházející z proudu 'Sport' mají předponu řetězce 'xyz' v prostoru tématu správce front verze 7. Publikování nebo přihlášení k odběru verze 7 s předponami 'Sport' témat 'xyz' s řetězcem tématu. Pokud publikování směřuje k odběrateli verze 6, předpona 'xyz' je odebrána z publikace a je umístěna v proudu produktu 'Sport'. A naopak, když publikování přechází z verze 6 na verzi 7, z proudu 'Sport' na téma 'Sport', je předpona 'xyz' přidána do řetězce tématu.



Obrázek 18. Proud verze 6, které koexistují s tématy verze 7

### Body odběru a témata

Bod odběru použitý k vyžádání publikování z konkrétní sady uzlů publikování v produktu WebSphere MQ Event Broker a Message Broker. Pojmenované body odběru jsou emulovány tématy a objekty témat.

The WebSphere MQ Event Broker V6.0 to WebSphere MQ V7.0.1 migration procedure, **migmbbrk**, converts named subscription points into topics and topic objects. Bod odběru se automaticky migruje, pokud má zachované publikování, nebo registrovaný odběratel. Příkaz **migmbbrk** vytváří objekty témat z pojmenovaných bodů odběru. Název bodu odběru se stane názvem objektu tématu a samotný řetězec tématu. Objekt tématu je přidán do produktu SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.

Pokud objekt tématu se stejným názvem již existuje, **migmbbrk** provede jednu ze dvou věcí.

1. Má-li objekt tématu jiný řetězec tématu, nebo pokud je název bodu odběru delší než název objektu, produkt **migmbbrk** vytvoří objekt tématu s generovaným názvem.
2. Pokud má objekt tématu stejný řetězec tématu, produkt **migmbbrk** přidá existující objekt do seznamu názvů.

Chcete-li přidat body odběru ručně, přečtěte si téma [Přidání bodu odběru](#).

## Body odběru v produktu WebSphere MQ Event Broker

Uzly publikování se používají v toku zpráv produktu WebSphere MQ Event a Message Broker k filtrování a odesílání zpráv odběratelům. Vydavatelé obvykle nenastavují body odběru na uzlech publikování. Odběratelé registrují zájem o konkrétní sadu témat a obvykle také neurčují body odběru.

Bod odběru je způsob, jak vybrat, které uzly publikování budou předávat zprávy odběru. Odběratel kvalifikuje svůj zájem o sadu témat s názvem bodu odběru.

Chcete-li nastavit název bodu odběru, přiřadte mu název vlastnosti produktu **Subscription point** uzlu publikování.

Vlastnost bodu odběru určuje, zda je publikování tématu přeměrováno odběratelům na stejné téma. Publikování z uzlů publikování s pojmenovaným bodem odběru se postupují pouze odběratelům na stejný bod odběru. Publikování z publikačních uzlů bez pojmenovaného bodu odběru, výchozí, jsou postoupeny pouze odběratelům, kteří nemají název bodu odběru.

Uzly s pojmenovaným bodem odběru odesílají zprávy příkazu Publish ve formátu MQRFH2 se sadou vlastností **SubPoint**. Odběry k pojmenovanému bodu odběru musí nastavit vlastnost **SubPoint** ve zprávě příkazu MQRFH2 Register subscriber.

## Body odběru v produktu WebSphere MQ

Produkt WebSphere MQ mapuje body odběru na různé prostory témat ve stromu témat produktu WebSphere MQ. Témata v příkazových zprávách bez bodu odběru se mapují nezměněna na kořen stromu témat WebSphere MQ a dědí vlastnosti z produktu SYSTEM.BASE.TOPIC.

Zprávy příkazů s bodem odběru se zpracovávají pomocí seznamu objektů témat v produktu SYSTEM.QPUBSUB.SUBPOINT.NAMELIST. Název bodu odběru ve zprávě příkazu je porovnán s řetězcem tématu pro každý objekt tématu v seznamu. Je-li nalezena shoda, je název bodu odběru předřazen do řetězce tématu jako uzel tématu. Téma dědí své vlastnosti z přidruženého objektu tématu, který se nachází v produktu SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.

Výsledkem použití bodů odběru je vytvoření samostatného prostoru tématu pro každý bod odběru. Prostor tématu je kořenem v tématu, které má stejný název jako bod odběru. Témata v každém prostoru tématu dědí vlastnosti z objektu tématu se stejným názvem, jako má bod odběru.

Jakékoli vlastnosti, které nejsou nastaveny ve vyhovujícím objektu tématu, jsou zděděny běžným způsobem z produktu SYSTEM.BASE.TOPIC.

Existující fronty publikování/odběru ve frontě pomocí záhlaví zpráv produktu MQRFH2 pokračují v práci nastavením vlastnosti **SubPoint** ve zprávách příkazu Publish nebo Register subscriber. Bod odběru je zkombinován s řetězcem tématu ve zprávě příkazu a výsledné téma je zpracováno stejně jako ostatní.

Nová aplikace WebSphere MQ V7 není ovlivněna body odběru. Pokud používá téma, které dědí z jednoho z odpovídajících objektů tématu, spolupracuje s aplikací ve frontě s použitím odpovídajícího bodu odběru.



## Příklad

Existující aplikace WebSphere MQ Event Broker publish/subscribe v kolektivu používá body odběru za účelem publikování cen akcií v různých měnách. Cena dolaru na burze IBM se publikuje s použitím bodu odběru USD a tématu NYSE/IBM/SPOT. Cena za vynikající cenu se zveřejňuje za použití stejného tématu a bodu odběru GBP.

Postup migrace v produktu WebSphere MQ vytváří dva objekty témat, GBP a USD, s odpovídajícími řetězci témat 'GBP' a 'USD'.

Existující vydavatelé k tématu NYSE/IBM/SPOT, migrovaný ke spuštění na serveru WebSphere MQ, který používá bod odběru USD, vytváří publikace na téma USD/NYSE/IBM/SPOT. Podobně existující odběratelé do produktu NYSE/IBM/SPOTs použitím bodu odběru USD vytvářejí odběry USD/NYSE/IBM/SPOT.

Přihlaste se k odběru ceny za dolar v programu publish/subscribe verze 7 tím, že zavolá MQSUB. Vytvořte odběr pomocí objektu tématu USD a řetězce tématu 'NYSE/IBM/SPOT', jak je ilustrováno v části kódu 'C'.

```
stncpy(sd.ObjectName, "USD", MQ_TOPIC_NAME_LENGTH);
sd.ObjectString.VSPtr = "NYSE/IBM/SPOT";
sd.ObjectString.VSLength = MQVS_NULL_TERMINATED;
MQSUB(Hconn, &sd, &Hobj, &Hsub, &CompCode, &Reason);
```

Zvažte, zda aplikace zprostředkovatele událostí produktu WebSphere MQ v kolektivu vždy používají body odběru USD a GBP. Pokud tomu tak je, vytvořte objekty tématu USD a GBP pouze jednou, jako témata klastru na hostiteli témat klastru. Nemusíte provádět krok [../com.ibm.mq.mig.doc/q007670\\_dita#q007670\\_/clusterstep](#) procedury migrace ke změně SYSTEM.BASE.TOPIC, na každém správci front v klastru, na téma klastru. Místo toho proveďte tyto kroky:

1. Nastavte atribut CLUSTER objektů témat USD a GBP na hostiteli témat klastru.
2. Odstraňte všechny kopie objektů tématu USD a GBP v ostatních správcích front v klastru.
3. Ujistěte se, že USD a GBP jsou definovány v SYSTEM.QPUBSUB.SUBPOINT.NAMELIST na každém správci front v klastru.

## Distribuované publikování/odběr

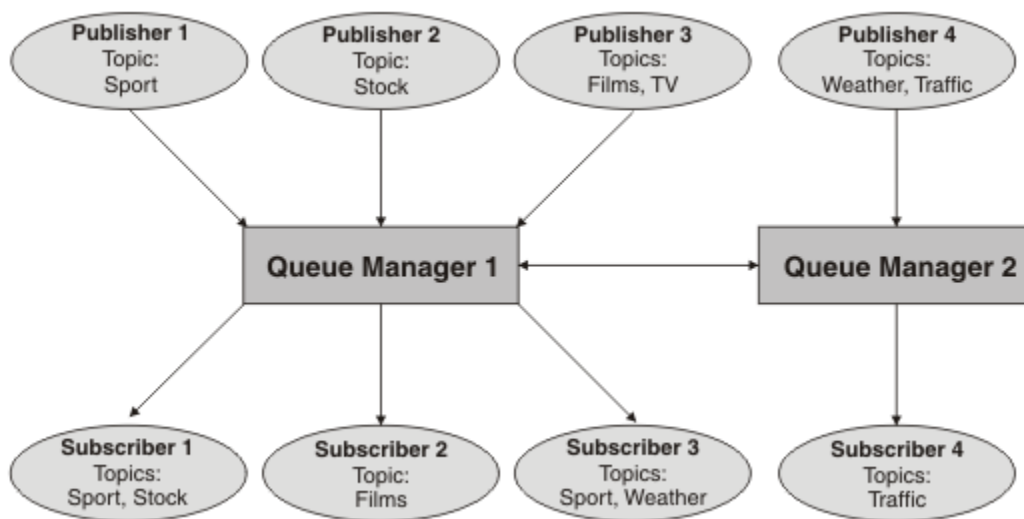
Tento oddíl obsahuje informace o tom, jak lze provádět systém zpráv publikování/odběru mezi správci front a dvěma různými topologiemi správce front, které lze použít k připojení správců front, klastrů a hierarchií.

Správci front mohou komunikovat s dalšími správci front v systému WebSphere MQ publish/subscribe, aby se odběratelé mohli přihlásit k odběru jednoho správce front a přijímat zprávy, které byly původně publikovány v jiném správci front. To je ilustrováno v tématu [Obrázek 19](#) na stránce 49.

[Obrázek 19](#) na stránce 49 zobrazuje systém publikování/odběru se dvěma správci front.

- Správce front 2 je používán produktem Publisher 4 k publikování informací o prognóze počasí pomocí tématu Počasí a informace o dopravních podmínkách na hlavních silnicích za použití tématu Provoz.
- Odběratel 4 také používá tohoto správce front a přihlašuje se k odběru informací o provozních podmínkách pomocí tématu Provoz.
- Odběratel 3 také odebírá informace o meteorologických podmínkách, i když používá jiného správce front od vydavatele. To je možné, protože jsou k sobě navzájem propojeny správce front.





Obrázek 19. Příklad publikování/odběru se dvěma správci front

### **Jak distribuovaná práce publikování/odběru funguje?**

Produkt WebSphere MQ publish/subscribe používá proxy odběry, aby bylo zajištěno, že odběratelé mohou přijímat zprávy, které jsou publikovány ve vzdálených správci front.

Distribuované publikování/odběr používá stejné komponenty jako distribuované řazení do front pro připojení síti správců front a následně k aplikacím, které se připojují k těmto správci front. Další informace o systému zpráv mezi správci front a komponentami, které se podílejí na vytváření připojení mezi správci front, naleznete v dokumentaci *Intercommunication*.

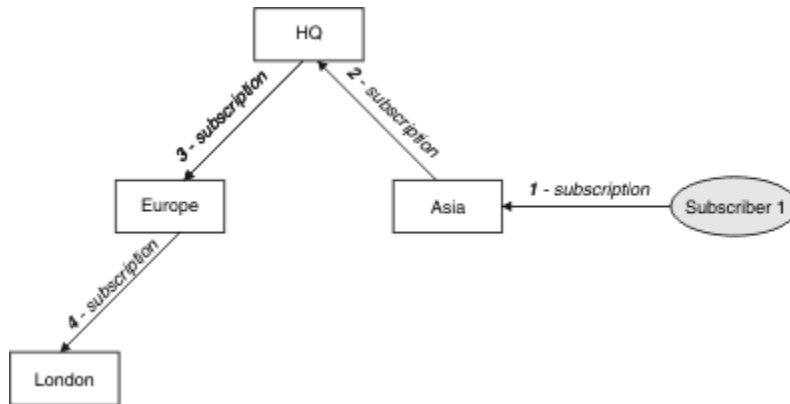
Odběratelé nemusí provádět nic kromě standardní operace odběru v distribuovaném systému publikování/odběr. Je-li odběr proveden ve správci front, spravuje správce front proces, kterým je odběr šířen do připojených správců front. Tok proxy odběrů směřuje ke všem správci front v síti. Vytvoří se, aby se zajistilo, že publikace budou přesměrovány zpět do správce front, ve kterém byl vytvořen původní odběr; viz [Obrázek 20 na stránce 50](#).

Publikování se šíří do vzdáleného správce front pouze v případě, že existuje odběr tohoto tématu v daném vzdáleném správci front.

Správce front konsoliduje všechny odběry, které jsou v ní vytvořeny, ať už z lokálních aplikací, nebo ze vzdálených správců front. Vytvoří proxy odběry pro témata odběrů se svými sousedy, pokud neexistuje odběr; viz [Obrázek 21 na stránce 50](#).

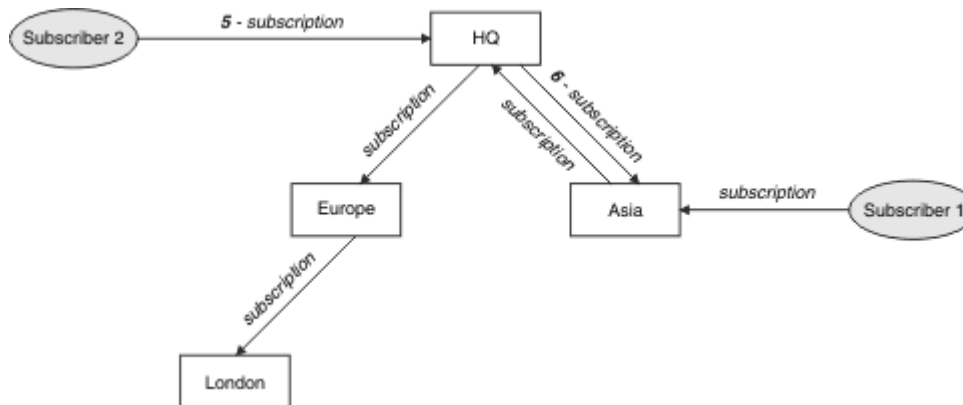
Když aplikace publikuje informace, přijímající správce front ji předá všem aplikacím, které mají platné odběry ve vzdálených správci front. Může ji předat prostřednictvím jednoho nebo více zprostředkujících správců front. Informace naleznete v tématu [Obrázek 22 na stránce 51](#).

Odběratel 1 registruje odběr pro konkrétní téma ve správci front Asia (1). Odběr pro toto téma je předáván všem ostatním správcům front v síti (2,3, 4).



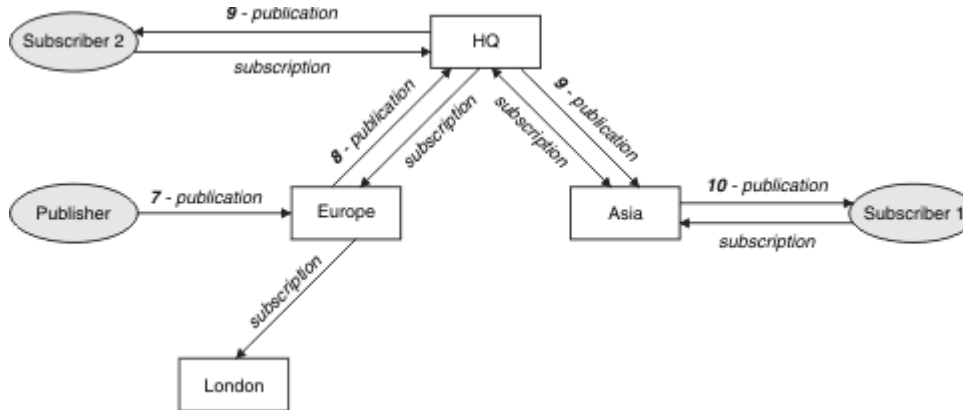
Obrázek 20. Šíření odběrů prostřednictvím sítě správce front

Odběratel 2 registruje odběr na stejné téma jako v produktu Obrázek 20 na stránce 50ve správci front HQ (5). Odběr pro toto téma je předáván správci front Asia, takže si je vědom toho, že odběry existují i jinde v síti (6). Odběr není přesměrován do správce front Europe, protože odběr pro toto téma již byl zaregistrován; viz krok 3 v příručce Obrázek 20 na stránce 50.



Obrázek 21. Více odběrů

Vydavatel odesílá publikování na stejné téma jako v produktu Obrázek 21 na stránce 50 do správce front Europe (7). Pro toto téma existuje odběr z ústředí do Evropy, takže je publikace předána správci front HQ (8). Od Londýna do Evropy však neexistuje žádný odběr (pouze z Evropy do Londýna), takže zveřejnění není přesměrováno do londýnského správce front. Správce front HQ posílá publikování přímo na odběratele 2 a do správce front Asia (9). Zveřejnění je předáno odběrateli 1 z Asie (10).



Obrázek 22. Šíření publikací prostřednictvím sítě správce front

Odešle-li správce front do jiného správce front publikace nebo odběry, nastaví vlastní ID uživatele ve zprávě. Pokud používáte hierarchii publikování/odběru a pokud je příchozí kanál nastaven tak, aby odesílal zprávy s oprávněním ID uživatele do zprávy, musíte autorizovat ID uživatele odesílajícího správce front; viz [“Použití výchozích ID uživatelů s hierarchií správce front”](#) na stránce 104. Pokud používáte klastry typu publikování-odběr, je autorizace zpracována klastrem.

Vzhledem k propojené povaze správců front publikování/odběru je nutné, aby se předplatná proxy propagují kolem všech uzlů v síti. Vzdálené publikace nemusí být okamžitě odebrány k odběru okamžitě. Odklad pro odběr můžete eliminovat použitím atributu **Topic** PROXYSUB s hodnotou FORCE, jak je popsáno v tématu [“Více o mechanismech směrování”](#) na stránce 52.

Operace odběru končí, když byl proxy odběr umístěn do příslušné přenosové fronty pro každého přímo připojeného správce front. Operace odběru nečeká na šíření odběru proxy na zbývající topologii.

Odběry proxy jsou přidruženy k názvu správce front, který je vytvořil. Mají-li správci front v hierarchii stejný název, může dojít k tomu, že se k nim nedostanou publikace. Chcete-li se tomuto problému vyhnout tak, jako je tomu u systému zpráv typu point-to-point, poskytněte správci front jedinečné názvy, zejména pokud jsou přímo nebo nepřímo propojeny v síti WebSphere MQ.

V rámci distribuované sítě publikování/odběru lze tok publikování a odběrů řídit, a je-li to vhodné, omezené, použití rozsahu publikování a odběru.

#### *Agregace odběru proxy a agregace publikování*

Publikování publikování/odběru publikování a proxy odběry jsou agregovány za účelem minimalizace množství zpráv předávaných mezi správci front publikování/odběru.

Proxy odběr je odběr vytvořený jedním správcem front pro témata publikován na jiném správci front. Proxy odběry explicitně nevytvoříte, správce front tak učiní ve vašem zastoupení; viz [“Jak distribuovaná práce publikování/odběru funguje?”](#) na stránce 49.

Správce front je možné připojit k hierarchii publikování/odběru nebo do klastru publikování/odběru. Průběh odběru proxy mezi připojenými správci front. Odběry proxy způsobí, že publikace k tématu vytvořenému vydavatelem připojeným k jednomu správci front obdrží odběratelé na toto téma připojené k jiným správcům front; viz [“Topologie publikování/odběru”](#) na stránce 61.

Proxy odběr probíhá mezi správci front pro každý jednotlivý řetězec tématu, k jehož odběru je přihlášen nějaký odběr.

Průtok proxy odběrů a publikování můžete omezit mezi propojenými správci front pomocí atributů **Topic PUBSCOPE** a **SUBSCOPE**. Tok proxy odběrů obsahující zástupné znaky můžete také omezit nastavením atributu **Topic WILDCARD** na hodnotu **BLOCK**; viz [“Pravidla zástupných znaků”](#) na stránce 54.

Odběry proxy jsou vtečené mezi správci front asynchronně k vytvoření odběrů. Můžete snížit latenci čekání na šíření proxy odběru na všechny připojené správce front nastavením atributu **Topic PROXYSUB** na **FORCE** v tématu nebo nadřazeným tématem tématu, které bude přihlášeno k odběru; viz [“Více o mechanismech směrování”](#) na stránce 52.

## Agregace odběru proxy

Odběry proxy jsou agregovány pomocí duplicitního eliminačního systému. Pro konkrétní vyřešený řetězec tématu je odeslán proxy odběr na prvním lokálním odběru nebo na přijatém proxy odběru. Další odběry stejného řetězce tématu budou používat tento existující odběr serveru proxy.

Odběr proxy je zrušen po zrušení posledního odběru lokálního odběru nebo přijetí proxy odběru.

V topologiích publikování/odběru s mnoha tisíci odběrů na jednotlivé řetězce témat nebo v případech, kdy existence těchto odběrů může být rychle změněna, je třeba zvážit režii šíření odběru proxy. Individuální proxy odběry mohou být konsolidovány prostřednictvím použití atributu tématu **PROXYSUB**, který je nastaven na **FORCE**. Další informace o mechanismech směrování a výkonu tématu klastru najdete v tématu [“Více o mechanismech směrování”](#) na stránce 52.

## Agregace publikací

Je-li ve správci front více než jeden odběr ze stejného řetězce tématu, bude z jiných správců front v topologii publikování/odběru odeslán z jiných správců front pouze jedna kopie každé publikace odpovídající tomuto řetězci tématu. Při přijetí zprávy lokální správce front doručí kopii zprávy každému odpovídajícímu odběru.

Je možné, aby více než jeden odběr proxy odpovídal řetězci tématu v rámci jediné publikace, když proxy odběry obsahují zástupné znaky. Je-li zpráva publikována ve správci front, který odpovídá dvěma nebo více odběrům proxy vytvořeným pomocí jednoho připojeného správce front, předá se vzdálenému správci front pouze jedna kopie publikování, aby bylo možné splnit více odběrů proxy.

### *Více o mechanismech směrování*

Volba *Publikovat všude* představuje alternativní mechanismus směrování pro individuální proxy odběr-předávání. Individuální přesměrování proxy odběru znamená, že do vzdáleného serveru systému zpráv se odešlou pouze publikování, která mají odpovídající odběr v řetězci tématu. Publikování na celém světě nebo vysílání funguje přesměrováním všech publikování, které jsou publikovány na server zasílání zpráv, na všechny ostatní servery zasílání zpráv v síti distribuovaných publikování/odběru. Přijímající servery zasílání zpráv pak doručí ty publikace, které odpovídají lokálním odběrům.

Každý mechanismus má své výhody, ale má také omezení.

### **Přesměrování jednotlivého odběru proxy**

Tento mechanismus vede k tomu, že je odeslán alespoň objem publikování mezi správci front, protože jsou odesílány pouze ty publikace, které odpovídají odběrům ve správci front.

Avšak:

- Každý jednotlivý řetězec tématu, který je přihlášen k odběru, vede k odběru proxy, který je odeslán všem ostatním správci front v topologii publikování/odběru. Tato režie systému zpráv může být významná, pokud existuje mnoho tisíc odběrů, které lze vytvořit nebo odstranit (například všechny netrvalé odběry po restartu správce front) nebo pokud se sada odběrů rychle mění a každý z nich má jiný řetězec tématu.
- Odběry proxy jsou vtečena do jiných správců front pomocí asynchronního systému zpráv, proto existuje prodleva mezi vytvořením odběru a doručení proxy odběru, doručení a zpracováním ostatními správci front. Zprávy, které jsou publikovány v těchto správcích front v daném intervalu, nebudou doručeny vzdálenému odběru.

## Publikovat všude

S tímto mechanismem:

- Na systému není žádná režie proxy řetězců proxy řetězců, což znamená rychlé vytvoření odběru, odstranění nebo změna nezpůsobí zvýšení zatížení sítě a zpracování.
- Mezi vytvářením odběru a publikacemi ve správci front nedochází k prodlevě, protože jsou vždy přenášena do všech správců front. Proto neexistuje žádné okno, kde by publikace nebyly doručeny do nově vytvořených vzdálených odběrů.

Avšak:

- Všechny publikace se posílají všem správcům front v topologii publikování/odběru, což může mít za následek nadměrný provoz na síti, kde publikování nemají ve všech správcích front odpovídající odběry.

Je možné, že budete chtít použít mechanismus publikování všude tam, kde očekáváte, že publikování bude odebíráno od významného podílu vašich správců front v klastru nebo hierarchii, nebo pokud jsou režie odběru proxy příliš velké kvůli frekvenci změn odběrů. Tato metoda práce může být v těchto instancích efektivnější než v jiných případech, kdy dochází ke zvýšenému provozu systému zpráv při odesílání publikací do všech správců front, nikoli na správce front s odpovídajícími odběry.

A publish everywhere mechanism can be enabled in IBM WebSphere MQ distributed publish/subscribe topologies by setting the **PROXYSUB** attribute to FORCE for a high-level topic object.

Podrobnosti o zakázání jednotlivých odběrů proxy naleznete v tématu [“Zakázání jednotlivých odběrů proxy”](#) na stránce 74.

Je-li tento vynucený proxy odběr šířen v rámci topologie, všechny nové odběry okamžitě přijímají všechna publikování od jiných připojených správců front, bez latence.

Při konfiguraci takového systému je třeba postupovat opatrně. Žádné objekty tématu pod tématem s **PROXYSUB** nastaveným na FORCE musí být v jiném klastru nebo v proudu hierarchie uzlu, kde je parametr **PROXYSUB** nastaven na hodnotu FORCE. Podobně, nižší objekty témat nesmí nastavit atribut **WILDCARD** na BLOK. V obou případech to může vést k tomu, že publikované zprávy netečou z jednoho správce front do jiného správce.

I když je parametr **PROXYSUB** nastaven na hodnotu FORCE, je odběr serveru proxy pro každý jednotlivý řetězec tématu, který je přihlášen k odběru, šířen dále. Je-li počet a četnost odběrů dostatečně vysoká, aby způsobila značnou režii systému, mohou být zakázána pro všechna témata ve správci front. Podrobnosti o zakázání jednotlivých odběrů proxy naleznete v tématu [“Zakázání jednotlivých odběrů proxy”](#) na stránce 74.

## Výběrové vysílání a latence odběru

Pro zachování odběru proxy lze použít latenci odběru a parametr PROXYSUB (FORCE).

Například existuje potenciální problém proxy odběru z QM\_B do QM\_A neprovedených poté, co jsou odpojeni všichni odběratelé. Tato situace nemusí být žádoucí, pokud vyžadujete, aby provoz výběrového vysílání pokračoval i v případě, že se ukončí připojení jednosměrového vysílání ke správci front. Výběrové vysílání pro produkt WebSphere MQ udržuje předplatné proxy na krátkou dobu, v případě, že se k novému odběrateli připojí, přidáním několika minut latence do každého odběru proxy, takže nejsou nepřipravené k okamžitému ukončení posledního odběratele.

Můžete také použít volbu PROXYSUB (FORCE) u daného tématu a zajistit tak, že nevyřízené předplatné proxy bude vždy nevyřízené. Je třeba zajistit, aby zprávy předávané ve frontách byly vyžadovány alespoň jedním odběratelem po většinu doby, kdy je odběr aktivní. Je-li nastavena hodnota PROXYSUB (FORCE), může být odeslán odběr serveru proxy před prvním lokálním odběrem nebo odběr serveru proxy a nebude zrušen ani po zrušení posledního odběru lokálního odběru nebo přijetí proxy odběru.

Pokud je odběr stále nevytvořen, lze k zajištění pokračování přenosu zpráv použít komunikaci typu P2P; další informace naleznete v tématu [Vysoká dostupnost pro výběrové vysílání](#).

### Pravidla zástupných znaků

Zástupné znaky v odběrech proxy se převádějí na použití zástupných znaků témat.

Je-li přijat odběr pro zástupný znak, může to být znak, který je používán produktem WebSphere MQ verze 6.0. Může se jednat také o téma, které používá produkt WebSphere Message Broker verze 6.0 a WebSphere MQ verze 7.0.

- Znakové zástupné znaky používají \* ke znázornění libovolného znaku, včetně / .
- Zástupné znaky tématu používají # k reprezentaci části prostoru tématu mezi znaky / .

V produktu WebSphere MQ verze 7.0 jsou všechny odběry proxy převedeny na zástupné znaky tématu. Je-li nalezen zástupný znak znaku, bude nahrazen znakem # , zpět na nejbližší / . Například /aaa/bbb/c\*d se převede na /aaa/bbb/#. Výsledky převodu ve vzdálených správčích front posílají o něco více publikací, než bylo explicitně upsána k odběru. Další publikace jsou odfiltrovány lokálním správcem front, když doručují publikace svým lokálním odběratelům.

## Řízení použití zástupného znaku s vlastností WILDCARD

Pomocí vlastnosti MQSC **Topic WILDCARD** nebo ekvivalentních vlastností PCF Topic `WildcardOperation` můžete řídit doručování příruček aplikacím, které používají řetězce názvů témat zástupných znaků. Vlastnost WILDCARD může mít jednu ze dvou možných hodnot:

### WILDCARD

Chování odběrů používajících zástupné znaky s ohledem na toto téma.

#### PASSTHRU

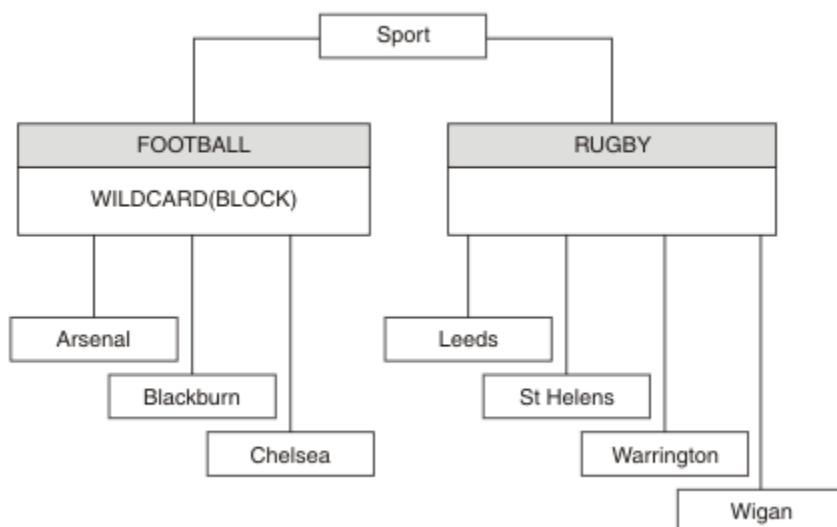
U odběrů registrovaných pro téma, které používá zástupné znaky a které je méně specifické než řetězec tématu v tomto objektu tématu, jsou poskytnuty publikace k tomuto tématu a k řetězcům tématu, které jsou specifičtější než toto téma.

#### BLOCK

U odběrů registrovaných pro téma, které používá zástupné znaky a které je méně specifické než řetězec tématu v tomto objektu tématu, nejsou poskytnuty publikace k tomuto tématu ani k řetězcům tématu, které jsou specifičtější než toto téma.

Hodnota tohoto atributu se použije při definici odběrů. Když tento atribut změníte, sada témat pokrytých existujícími odběry nebude touto změnou ovlivněna. Tento scénář platí i v případě, že se změnila topologie, tj. když byly objekty tématu vytvořeny nebo odstraněny. Sada témat odpovídajících odběrům, které byly vytvořeny po této změně atributu WILDCARD, se vytvoří s použitím této nové, upravené topologie. Pokud chcete vynutit opětovné vyhodnocení odpovídající sady témat pro existující odběry, musíte restartovat správce front.

V příkladu, [“Příklad: Vytvoření klastru pro publikování/odběr produktu Sport”](#) na stránce 42, můžete postupovat podle kroků k vytvoření stromové struktury témat, která je zobrazena v části [Obrázek 10](#) na stránce 38.



Obrázek 23. Strom témat, který používá vlastnost WILDCARD , BLOCK .

Odběratel používající řetězec tématu s zástupnými znaky # přijímá všechny publikace k tématu Sport a podstromu Sport /Rugby . Odběratel neobdrží žádné publikace do podstromu Sport/Football , protože hodnota vlastnosti WILDCARD u tématu Sport/Football je BLOCK.

Výchozí nastavení je PASSTHRU . Hodnotu vlastnosti ZÁSTUPNÝ ZNAK PASSTHRU můžete nastavit na uzly ve stromu Sport . Pokud uzly nemají hodnotu vlastnosti WILDCARD BLOCK, nastavení PASSTHRU nezmění chování pozorované odběratelem na uzlech ve stromu Sports .

V tomto příkladu vytvořte odběry a zjistěte, jak nastavení zástupných znaků ovlivňuje doručené publikace, viz Obrázek 14 na stránce 43. Spusťte publikační příkaz v produktu Obrázek 17 na stránce 44 a vytvořte některé publikace.

pub QMA

Obrázek 24. Publikovat na QMA

Výsledky jsou zobrazeny v Tabulka 3 na stránce 38. Všimněte si, jak nastavení hodnoty vlastnosti WILDCARD BLOCK brání odběrům se zástupnými znaky z příjmu publikací na témata v rámci rozsahu zástupného znaku.

Tabulka 6. Publikace přijaté v systému QMA

Předplatně	Řetězec tématu	Přijaté publikace	Poznámky
SPORTS	Sports/#	Sports Sports/Rugby Sports/Rugby/Leeds	Všechny publikace ve fotbalovém podstromu blokováné uživatelem WILDCARD (BLOCK) v systému Sports/Football
SARSENAL	Sports/#/Arsenal	-	WILDCARD (BLOCK) v Sports/ Football zabraňuje odběru zástupného znaku na Arsenal
SLEEDS	Sports/#/Leeds	Sports/Rugby/Leeds	Předvolba WILDCARD na Sports/ Rugby nezabrání odběru zástupného znaku na Leeds.

**Poznámka:**



Předpokládejme, že odběr má zástupný znak, který odpovídá objektu tématu s hodnotou vlastnosti WILDCARD BLOCK. Má-li odběr také řetězec tématu napravo od odpovídajícího zástupného znaku, odběr nikdy neobdrží publikování. Sada publikací, které nejsou blokovány, jsou publikace k tématům, která jsou nadřazenými prvky blokováného zástupného znaku. Publikování do témat, která jsou podřízenými prvky tématu s hodnotou vlastnosti produktu BLOCK, jsou blokovány zástupnými znaky. Proto řetězce témat odběru, které obsahují téma napravo od zástupného znaku, nikdy nepřijímají žádné publikace, které by se shodovaly.

Nastavení hodnoty vlastnosti WILDCARD na hodnotu BLOCK neznamena, že se nemůžete přihlásit k odběru pomocí řetězce tématu, který obsahuje zástupné znaky. Takové předplatné je normální. Odběr má explicitní téma, které odpovídá danému tématu s objektem tématu, který má hodnotu vlastnosti WILDCARD BLOCK. Používá zástupné znaky pro témata, která jsou nadřazenými nebo podřízenými prvky tématu s hodnotou vlastnosti WILDCARD BLOCK. V příkladu v produktu Obrázek 10 na stránce 38 může odběr, jako je Sports/Football/#, přijímat publikování.

## Zástupné znaky a témata klastru

Definice témat klastru jsou šířeny do všech správců front v klastru. Odběr tématu klastru v jednom správci front v klastru má za následek vytvoření proxy odběrů ve správci front. Proxy odběr je vytvořen ve všech ostatních správci front v klastru. Odběry pomocí řetězců témat obsahujících zástupné znaky, kombinované s tématy klastru, mohou být obtížné předpovědět chování. Chování je vysvětleno v následujícím příkladu.

V klastru nastavenými pro tento příklad, "Příklad: Vytvoření klastru pro publikování/odběr produktu Sport" na stránce 42, má QMB stejnou sadu odběrů jako QMA, ale QMB nepřijal žádné publikace poté, co vydavatel publikován na QMA, viz Obrázek 11 na stránce 38. Ačkoli témata Sports/Football a Sports/Rugby jsou témata klastru, odběry definované v souboru fullsubs.tst se neodkazují na téma klastru. Z produktu QMB do produktu QMA nejsou šířeny žádné odběry proxy. Bez odběrů proxy jsou do produktu QMB předávány žádné publikace QMA.

Některé odběry, jako např. Sports/#/Leeds, se mohou v tomto případě odkazovat na téma klastru Sports/Rugby. Odběr produktu Sports/#/Leeds je ve skutečnosti interpretováno jako objekt tématu SYSTEM.BASE.TOPIC.

Pravidlo pro vyřešení objektu tématu, na který se odkazuje odběr, jako je například Sports/#/Leeds, je následující. Ořízněte řetězec tématu na první zástupný znak. Skenování bylo ponecháno přes řetězec tématu, který hledá první téma, které má přidružený objekt administrativního tématu. Objekt tématu může určovat název klastru, nebo definovat lokální objekt tématu. V příkladu, Sports/#/Leeds, řetězec tématu po oseknutí je Sports, který nemá žádný objekt tématu, a tak se Sports/#/Leeds dědí od SYSTEM.BASE.TOPIC, což je lokální objekt tématu.

Chcete-li zjistit, jak může přihlášení k odběru klastrovaných témat změnit způsob, jakým šíření zástupných znaků funguje, spusťte dávkový skript upsubs.bat. Skript vymaže fronty odběru a přidá odběry témat klastru do adresáře fullsubs.tst. Znovu spusťte soubor puba.bat a vytvořte dávku publikací; viz Obrázek 11 na stránce 38.

Produkt Tabulka 4 na stránce 40 zobrazuje výsledek přidání dvou nových odběrů do stejného správce front, ve kterém byly publikovány publikace. Výsledkem je podle očekávání, že nové odběry obdrží jedno publikování a počty publikování přijatých ostatními odběry budou nezměněny. Dojde k neočekávaným výsledkům na druhém správci front klastru, viz Tabulka 5 na stránce 40.

Předplatné	Řetězec tématu	Přijaté publikace	Poznámky
SPORTS	Sports/#	Sports Sports/Rugby Sports/Rugby/Leeds	Všechny publikace ve fotbalovém podstromu blokováné uživatelem WILDCARD (BLOCK) v systému Sports/Football



Tabulka 7. Publikace přijaté v systému QMA (pokračování)

Předplatně	Řetězec tématu	Přijaté publikace	Poznámky
SARSENAL	Sports/#/Arsenal	-	WILDCARD (BLOCK) v Sports/Football zabraňuje odběru zástupného znaku na Arsenal
SLEEDS	Sports/#/Leeds	Sports/Rugby/Leeds	Předvolba WILDCARD na Sports/Rugby nezabrání odběru zástupného znaku na Leeds.
FARSENAL	Sports/Football/Arsenal	Sports/Football/Arsenal	Produkt Arsenal obdrží publikování, protože odběr nemá zástupný znak.
FLEEDS	Sports/Rugby/Leeds	Sports/Rugby/Leeds	Leeds obdrží publikování v každém případě.

Produkt Tabulka 5 na stránce 40 zobrazuje výsledky přidání dvou nových odběrů v produktu QMB a publikování v produktu QMA. Připomeňme si, že produkt QMB nepřijal žádná publikování bez těchto dvou nových odběrů. Jak bylo očekáváno, tyto dva nové odběry přijímají publikace, protože Sports/FootBall a Sports/Rugby jsou obě témata klastru. QMB postoupil proxy odběry pro Sports/Football/Arsenal a Sports/Rugby/Leeds do QMA, které následně odeslaly publikace do QMB.

Neočekávaný výsledek je takový, že se dva odběry Sports/# a Sports/#/Leeds, které dříve neobdržely žádné publikace, nyní přijímají publikace. Důvodem je to, že publikace Sports/Football/Arsenal a Sports/Rugby/Leeds předané produktu QMB pro ostatní odběry jsou nyní k dispozici pro všechny odběratele připojené k produktu QMB. V důsledku toho se odběry lokálních témat Sports/# a Sports/#/Leeds přijímají v publikaci Sports/Rugby/Leeds. Produkt Sports/#/Arsenal nadále neobdrží publikování, protože sport/fotbal má nastavenou hodnotu vlastnosti WILDCARD nastavenou na hodnotu BLOCK.

Tabulka 8. Publikace přijaté v systému QMB

Předplatně	Řetězec tématu	Přijaté publikace	Poznámky
SPORTS	Sports/#	Sports/Rugby/Leeds	Všechny publikace ve fotbalovém podstromu blokovány produktem WILDCARD (BLOCK) v systému Sports/Football
SARSENAL	Sports/#/Arsenal	-	WILDCARD (BLOCK) v Sports/Football zabraňuje odběru zástupného znaku na Arsenal
SLEEDS	Sports/#/Leeds	Sports/Rugby/Leeds	Výchozí hodnota WILDCARD na Sports/Rugby nezabrání odběru zástupných znaků v systému Leeds.
FARSENAL	Sports/Football/Arsenal	Sports/Football/Arsenal	Produkt Arsenal obdrží publikování, protože odběr nemá zástupný znak.
FLEEDS	Sports/Rugby/Leeds	Sports/Rugby/Leeds	Leeds obdrží publikování v každém případě.

Ve většině aplikací je nežádoucí pro jeden odběr ovlivnit chování jiného odběru. Jedno důležité použití vlastnosti WILDCARD s hodnotou BLOCK znamená, že se odběry ke stejnému řetězci tématu, které obsahují zástupné znaky, budou chovat jednotně. Údaj o tom, zda je odběr ve stejném správcí front jako vydavatel nebo jiný, výsledky odběru jsou stejné.

## Zástupné znaky a proudy

Proudy produktu WebSphere MQ verze 6 jsou mapovány na témata prostřednictvím produktu WebSphere MQ verze 7; viz [“Proudy a témata”](#) na stránce 44 . Ve výchozím mapování, které je provedeno produktem **strmqbrk** ve verzi 7, by všechna témata v proudu Sports byla mapována na téma Sports. Všechna témata v proudu Business budou mapována na téma Business.

Odběr v produktu WebSphere MQ verze 6 až \* v proudu produktu Sports přijímá všechny publikace ve stromu Sports a ve stromu Business nejsou k dispozici žádné publikace. Stejný odběr ve verzi 7 by přijímal všechny publikace ve stromu Sports a ve všech publikacích ve stromu Business . K zablokování tohoto chování, když jsou proudy migrovány do verze 7, produkt **strmqbrk** nastaví vlastnost WILDCARD . Nastaví ji na hodnotu BLOCK pro každé z témat nejvyšší úrovně, které jsou migrovány z proudu. Vlastnost WILDCARD produktu Sports a Business je nastavena na hodnotu BLOCK podle převodu z proudů verze 6 s názvem Sports a Business.

Pro novou aplikaci napsanou na rozhraní API pro publikování/odběr je výsledkem, že odběr z produktu \* neobdrží žádné publikace. Chcete-li přijmout všechny sportovní publikace, musíte se přihlásit k odběru produktu Sports/\*nebo produktu Sports/# a podobně jako publikace Business .

Chování existující aplikace publikování/odběru ve frontě se při migraci zprostředkovatele publikování/odběru do produktu WebSphere MQ verze 7 nezmění. Vlastnost **StreamName** v příkazech **Publish**, **Register Publisher**nebo **Subscriber** je mapována na název tématu, na který byl proud migrován.

## Zástupné znaky a body odběru

WebSphere body odběrů zprostředkovatele zpráv jsou mapovány na témata pomocí produktu WebSphere MQ verze 7; viz [“Body odběru a témata”](#) na stránce 46. Ve výchozím mapování, které je provedeno produktem **migmqbrk** ve verzi 7, by všechna témata v bodu odběru Sports byla mapována na téma Sports. Všechna témata v bodu odběru Business by byla mapována na téma Business.

Odběr produktu WebSphere Message Broker verze 6 na \* v bodu odběru Sports přijímá všechny publikace ve stromu Sports a ve stromu Business nejsou žádné publikace. Stejný odběr ve verzi 7 by přijímal všechny publikace ve stromu Sports a ve všech publikacích ve stromu Business . Chcete-li blokovat toto chování, při migraci bodů odběru na verzi 7 nastaví produkt **migmqbrk** vlastnost WILDCARD . Nastaví ji na hodnotu BLOCK pro každé z témat nejvyšší úrovně, které jsou migrovány z bodu odběru. Vlastnost WILDCARD produktu Sports a Business je nastavena na hodnotu BLOCK převodem z bodů odběru produktu WebSphere Message Broker s názvem Sports a Business .

U nové aplikace napsané pro rozhraní API pro publikování/odběr je výsledkem migrace skutečnost, že odběr produktu \* přijímá žádné publikace. Chcete-li přijmout všechny sportovní publikace, musíte se přihlásit k odběru produktu Sports/\*nebo produktu Sports/# a podobně jako publikace Business .

Chování existující aplikace publikování/odběru ve frontě se při migraci zprostředkovatele publikování/odběru do produktu WebSphere MQ verze 7 nezmění. Vlastnost **SubPoint** v příkazech **Publish**, **Register Publisher**nebo **Subscriber** je mapována na název tématu, na které byl odběr migrován.

### Příklad: Vytvoření klastru pro publikování/odběr produktu Sport

Kroky následující po vytvoření klastru CL1se čtyřmi správci front: dvě úplná úložiště, CL1A a CL1B a dvě dílčí úložiště, QMA a QMB. Úplná úložiště se používají k zadržení pouze definic klastru. QMA je označen jako hostitel tématu klastru. Trvalé odběry jsou definovány na serveru QMA i v produktu QMB.

**Poznámka:** Příklad je kódován pro systém Windows. Chcete-li nakonfigurovat a otestovat tento příklad na jiných platformách, musíte soubor [Create qmgrs.bat](#) a [create pub.bat](#) nakonfigurovat a otestovat.

1. Vytvořte skriptové soubory.
  - a. [Vytvoření topics.tst](#)
  - b. [Vytvořit wildsubs.tst](#)
  - c. [Vytvořit fullsubs.tst](#)
  - d. [Vytvořit qmgrs.bat](#)

e. `create pub.bat`

2. Chcete-li vytvořit konfiguraci, spusťte příkaz `Create qmgrs.bat` .

```
qmgrs
```

Vytvořte témata v produktu Obrázek 10 na stránce 38. Skript na obrázku 5 vytvoří témata klastru `Sports/Football` a `Sports/Rugby`.

**Poznámka:** Volba `REPLACE` nenahrazuje vlastnosti typu `TOPICSTR` v rámci tématu. `TOPICSTR` je vlastnost, která se používá v příkladu k testování různých stromů témat. Chcete-li změnit témata, odstraňte nejprve téma.

```
DELETE TOPIC ('Sports')
DELETE TOPIC ('Football')
DELETE TOPIC ('Arsenal')
DELETE TOPIC ('Blackburn')
DELETE TOPIC ('Chelsea')
DELETE TOPIC ('Rugby')
DELETE TOPIC ('Leeds')
DELETE TOPIC ('Wigan')
DELETE TOPIC ('Warrington')
DELETE TOPIC ('St. Helens')

DEFINE TOPIC ('Sports')      TOPICSTR('Sports')
DEFINE TOPIC ('Football')   TOPICSTR('Sports/Football') CLUSTER(CL1) WILDCARD(BLOCK)
DEFINE TOPIC ('Arsenal')    TOPICSTR('Sports/Football/Arsenal')
DEFINE TOPIC ('Blackburn')  TOPICSTR('Sports/Football/Blackburn')
DEFINE TOPIC ('Chelsea')    TOPICSTR('Sports/Football/Chelsea')
DEFINE TOPIC ('Rugby')      TOPICSTR('Sports/Rugby') CLUSTER(CL1)
DEFINE TOPIC ('Leeds')      TOPICSTR('Sports/Rugby/Leeds')
DEFINE TOPIC ('Wigan')      TOPICSTR('Sports/Rugby/Wigan')
DEFINE TOPIC ('Warrington') TOPICSTR('Sports/Rugby/Warrington')
DEFINE TOPIC ('St. Helens') TOPICSTR('Sports/Rugby/St. Helens')
```

*Obrázek 25. Odstraňte a vytvořte témata: `topics.tst`*

**Poznámka:** Odstraňte témata, protože produkt `REPLACE` nebude nahrazovat řetězce témat.

Vytvoření odběrů se zástupnými znaky. Zástupné znaky odpovídají tématům s objekty témat v produktu Obrázek 10 na stránce 38. Vytvořte frontu pro každý odběr. Fronty jsou vymazány a odběry odstraněny, když je skript spuštěn nebo znovu spuštěn.

**Poznámka:** Volba `REPLACE` nenahrazuje vlastnosti `TOPICOBJ` nebo `TOPICSTR` odběru. `TOPICOBJ` nebo `TOPICSTR` jsou vlastnosti, které jsou užitečné v příkladu pro testování různých odběrů. Chcete-li je změnit, nejprve odstraňte odběr.

```
DEFINE QLOCAL(QSPORTS) REPLACE
DEFINE QLOCAL(QSARSENAL) REPLACE
DEFINE QLOCAL(QSLEEDS) REPLACE
CLEAR QLOCAL(QSPORTS)
CLEAR QLOCAL(QSARSENAL)
CLEAR QLOCAL(QSLEEDS)

DELETE SUB (SPORTS)
DELETE SUB (SARSENAL)
DELETE SUB (SLEEDS)
DEFINE SUB (SPORTS) TOPICSTR('Sports/#') DEST(QSPORTS)
DEFINE SUB (SARSENAL) TOPICSTR('Sports+/Arsenal') DEST(QSARSENAL)
DEFINE SUB (SLEEDS) TOPICSTR('Sports+/Leeds') DEST(QSLEEDS)
```

*Obrázek 26. Vytvoření zástupných znaků pro zástupný znak: `wildsubs.tst`*

Vytvořte odběry, které odkazují na objekty tématu klastru.

**Poznámka:**

Oddělovač, /, se automaticky vkládá mezi řetězec tématu, na který odkazuje `TOPICOBJ`, a řetězec tématu definovaný parametrem `TOPICSTR`.

Definice `DEFINE SUB(FARSENAL) TOPICSTR('Sports/Football/Arsenal') DEST(QFARSENAL)` vytváří stejný odběr. `TOPICOBJ` se používá jako rychlý způsob, jak odkazovat na řetězec tématu, který jste již definovali. Když se odběr vytvoří, již se nebude odkazovat na objekt tématu.

```
DEFINE QLOCAL(QFARSENAL) REPLACE
DEFINE QLOCAL(QRLEEDS) REPLACE
CLEAR QLOCAL(QFARSENAL)
CLEAR QLOCAL(QRLEEDS)

DELETE SUB (FARSENAL)
DELETE SUB (RLEEDS)
DEFINE SUB (FARSENAL) TOPICOBJ('Football') TOPICSTR('Arsenal') DEST(QFARSENAL)
DEFINE SUB (RLEEDS) TOPICOBJ('Rugby') TOPICSTR('Leeds') DEST(QRLEEDS)
```

Obrázek 27. Odstraňte a vytvořte odběry: `fullsubs.tst`

Vytvořte klastr se dvěma úložišti. Vytvořte dvě dílčí úložiště pro publikování a odběr. Znovu spusťte skript k odstranění všeho a začněte znovu. Skript také vytvoří hierarchii témat a počáteční zástupné znaky odběrů.

#### Poznámka:

Na ostatních platformách napište podobný skript nebo zadejte všechny příkazy. Pomocí skriptu lze rychle odstranit vše a začít znovu se stejnou konfigurací.

```
@echo off
set port.CL1B=1421
set port.CL1A=1420
for %%A in (CL1A CL1B QMA QMB) do call :createQM %%A
call :configureQM CL1A CL1B %port.CL1B% full
call :configureQM CL1B CL1A %port.CL1A% full
for %%A in (QMA QMB) do call :configureQM %%A CL1A %port.CL1A% partial
for %%A in (topics.tst wildsubs.tst) do runmqsc QMA < %%A
for %%A in (wildsubs.tst) do runmqsc QMB < %%A
goto:eof

:createQM
echo Configure Queue manager %1
endmqm -p %1
for %%B in (dlt crt str) do %%Bmqm %1
goto:eof

:configureQM
if %1==CL1A set p=1420
if %1==CL1B set p=1421
if %1==QMA set p=1422
if %1==QMB set p=1423
echo configure %1 on port %p% connected to repository %2 on port %3 as %4 repository
echo DEFINE LISTENER(LST%1) TRPTYPE(TCP) PORT(%p%) CONTROL(QMGR) REPLACE | runmqsc %1
echo START LISTENER(LST%1) | runmqsc %1
if full==%4 echo ALTER QMGR REPOS(CL1) DEADQ(SYSTEM.DEAD.LETTER.QUEUE) | runmqsc %1
echo DEFINE CHANNEL(TO.%2) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('LOCALHOST(%3)') CLUSTER(CL1)
REPLACE | runmqsc %1
echo DEFINE CHANNEL(TO.%1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('LOCALHOST(%p%)')
CLUSTER(CL1) REPLACE | runmqsc %1
goto:eof
```

Obrázek 28. Vytvoření správců front: `qmgrs.bat`

Aktualizujte konfiguraci přidáním odběrů do témat klastru.

```
@echo off
for %%A in (QMA QMB) do runmqsc %%A < wildsubs.tst
for %%A in (QMA QMB) do runmqsc %%A < upsubs.tst
```

Obrázek 29. Aktualizovat odběry: `upsubs.bat`

Spuštěním příkazu `pub.bat` se správcem front jako parametrem publikujete zprávy obsahující řetězec tématu publikování. Produkt `Pub.bat` používá vzorový program **amqspub**.

```
@echo off
@rem Provide queue manager name as a parameter
set S=Sports
set S=6 Sports/Football Sports/Football/Arsenal
set S=6 Sports/Rugby Sports/Rugby/Leeds
for %%B in (6) do echo %%B | amqspub %%B %1
```

Obrázek 30. Publikovat: pub.bat

### Topologie publikování/odběru

Topologie publikování/odběru se skládá z správců front a spojení mezi nimi, které podporují aplikace publikování/odběru.

Aplikace typu publikování/odběr se může skládat ze sítě správců front, kteří jsou připojeni. Správci front se mohou všichni nacházet ve stejném fyzickém systému nebo mohou být distribuovány přes několik fyzických systémů. Připojením správců front k aplikaci může aplikace přijímat publikování s použitím libovolného správce front v síti.

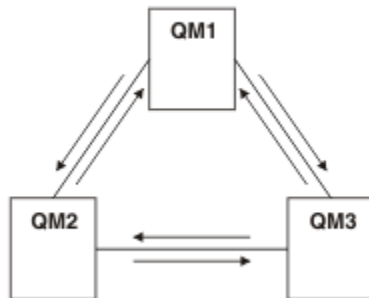
To poskytuje následující výhody:

- Klientské aplikace mohou komunikovat s blízkým správcem front, nikoli se vzdáleným správcem front, a tím dosáhnout lepších dob odezvy.
- Při použití více než jednoho správce front je možné více odběratelů podporovat.

Můžete uspořádat správce front, kteří provádějí systém zpráv publikování/odběru ve dvou různých způsobech, klastrech a hierarchiích. Příklady jednoduchého klastru a jednoduché hierarchie naleznete v tématu Obrázek 31 na stránce 61 a Obrázek 32 na stránce 62. Další informace o těchto dvou topologiích a zjištění, které z těchto dvou topologií je nejvhodnější, naleznete v informacích v této části dokumentace k produktu.

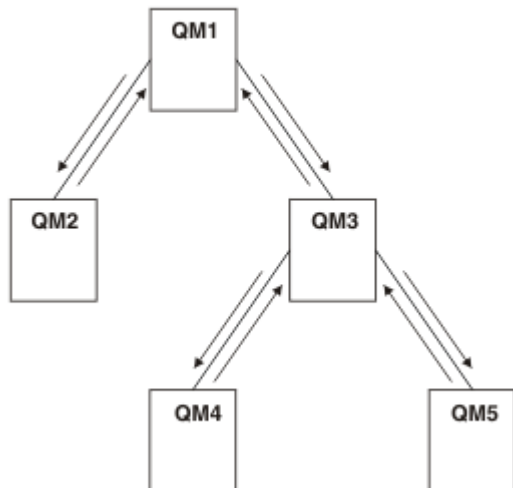
Je možné použít obě topologie v kombinaci tak, že se spojí klastry společně v hierarchii.

#### Cluster



Obrázek 31. Klastř jednoduchého publikování/odběru

## Hierarchy



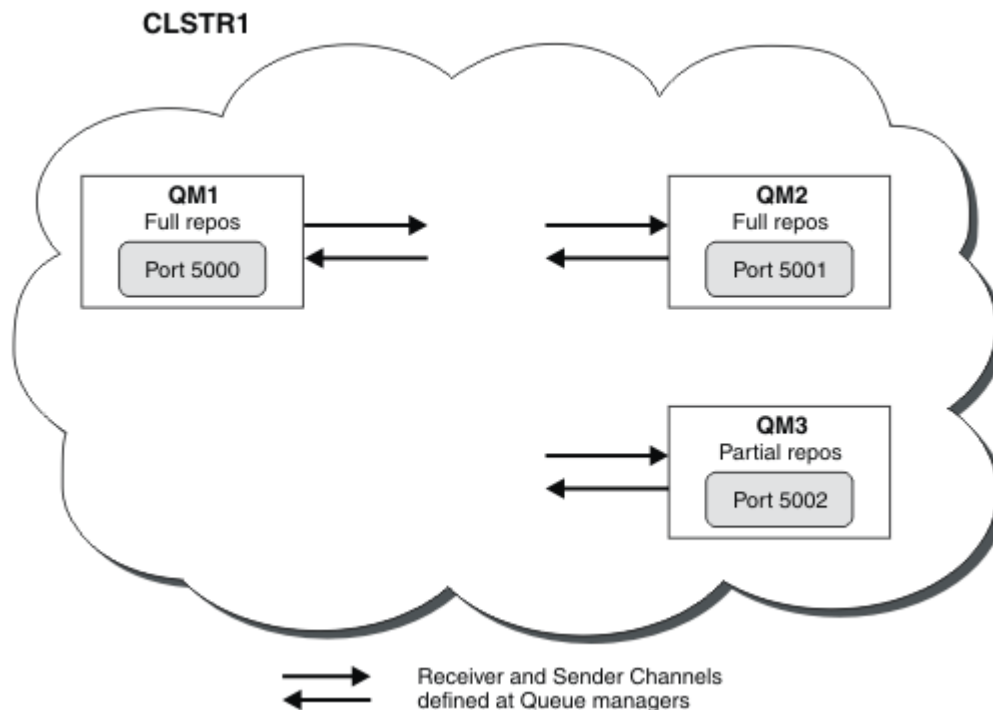
Obrázek 32. Jednoduchá hierarchie publikování/odběru

Nastavení klastru pro publikování/odběr: Scénář 1

Přidejte dva správce front jako úplná úložiště do klastru a definujte kanály mezi nimi.

## Informace o této úloze

Následující diagram má tři správce front: QM1 ,



QM2a QM3:

QM1 a QM2 jsou úplná úložiště v klastru a produkt QM3 je dílčí úložiště.

Scénář 1 přidá QM1 a QM2 do klastru DEMO jako úplná úložiště.

Scénář 2 přidává QM3 do klastru DEMO jako částečné úložiště.

Tyto úlohy vyžadují alespoň jedno příkazové okno.

## Postup

1. Nastavte QM1 a QM2 jako úplná úložiště klastru DEMO :

```
alter QMGR REPOS(DEMO)
```

2. Definujte a spusťte modul listener pro produkt QM1:

```
define listener(QM1_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(5000)
start listener(QM1_LS)
```

3. Definujte a spusťte modul listener pro produkt QM2:

```
define listener(QM2_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(5001)
start listener(QM2_LS)
```

4. Definujte přijímací kanál pro QM1:

```
DEFINE CHANNEL(DEMO.QM1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5000)')
CLUSTER(DEMO) DESCR('TCP Cluster-receiver channel for queue manager QM1')
```

5. Definujte odesílací kanál z QM1 na QM2:

```
DEFINE CHANNEL(DEMO.QM2) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5001)')
CLUSTER(DEMO) DESCR('TCP Cluster-sender channel from QM1 to queue manager QM2')
```

6. Definujte přijímací kanál pro QM2:

```
DEFINE CHANNEL(DEMO.QM2) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5001)')
CLUSTER(DEMO) DESCR('TCP Cluster-receiver channel for queue manager QM2')
```

7. Definujte odesílací kanál z QM2 na QM1:

```
DEFINE CHANNEL(DEMO.QM1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5000)')
CLUSTER(DEMO) DESCR('TCP Cluster-sender channel from qm2 to qm1')
```

8. Definujte téma klastru scores v systému QM1:

```
define topic(scores) TOPICSTR(/football) CLUSTER(DEMO)
```

9. Ověřte nastavení pomocí následujících příkazů:

```
display topic(scores) type(all) clusinfo
display clusqmgr(*)
display chstatus(*)
```

10. Otestujte nastavení pomocí dvou příkazových oken:

- a. Zadejte tento příkaz do prvního příkazového okna:

```
/opt/mqm/samp/bin/amqspub /FOOTBALL/scores QM1
```

- b. Zadejte tento příkaz do druhého příkazového okna:

```
/opt/mqm/samp/bin/amqssub /FOOTBALL/scores QM2
```

## Související úlohy

[Správa klastrů WebSphere MQ](#)

[Nastavení nového klastru](#)

*Nastavení klastru pro publikování/odběr: Scénář 2*

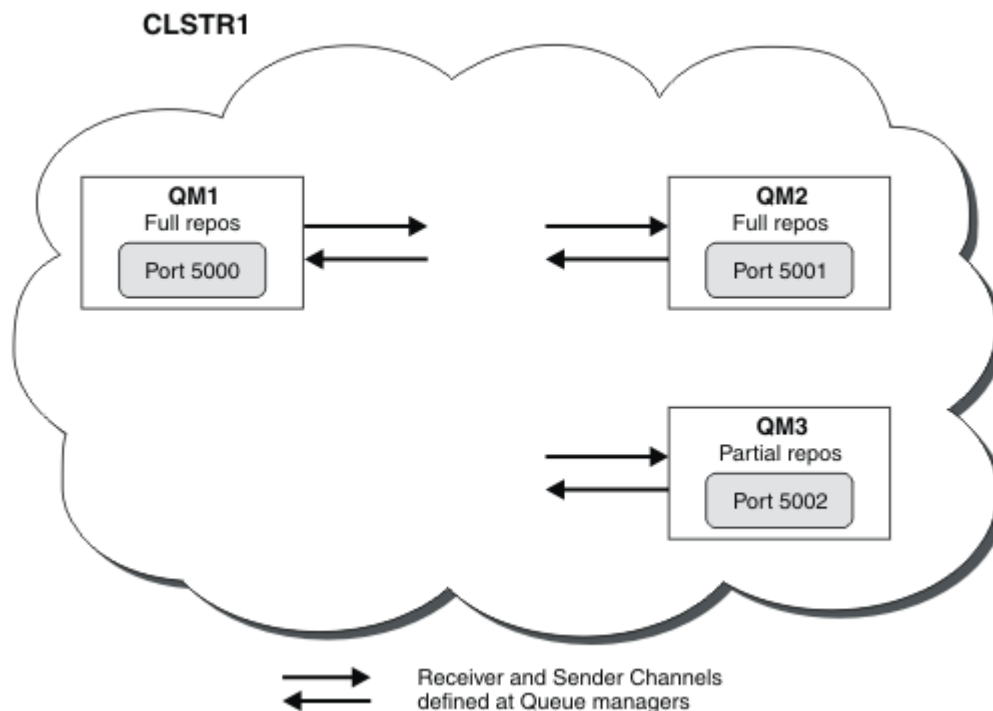
Přidejte třetího správce front jako dílčí úložiště do klastru.

## Než začnete

Před provedením této úlohy musí být úloha dokončena v produktu [“Nastavení klastru pro publikování/odběr: Scénář 1”](#) na stránce 62 .

## Informace o této úloze

Následující diagram má 3 správce front; QM1,



QM2a QM3:

QM1 a QM2 jsou úplná úložiště v klastru a produkt QM3 je dílčí úložiště.

Scenář 1 přidává QM1 a QM2 do klastru DEMO jako úplná úložiště.

Scenář 2 přidá QM3 do klastru DEMO jako dílčí úložiště.

Tyto úlohy vyžadují alespoň jedno příkazové okno.

## Postup

1. Definujte a spusťte modul listener pro produkt QM3:

```
define listener(QM3_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(5002)
start listener(QM3_LS)
```

2. Definujte přijímací kanál pro QM3:

```
DEFINE CHANNEL(DEMO.QM3) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5002)') CLUSTER
(DEMO) DESCR('TCP Cluster-receiver channel for queue manager QM3')
```

3. Definujte odesílací kanál z QM3 na QM1:

```
DEFINE CHANNEL(DEMO.QM1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5000)')
CLUSTER(DEMO) DESCR('TCP Cluster-sender channel from qm3 to qm1')
```

4. Ověřte nastavení pomocí následujících příkazů:

```
display topic(scores) type(all) clusinfo
display clusqmgr(*)
display chstatus(*)
```

5. Otestujte nastavení pomocí 2 příkazových oken:

- a. Zadejte tento příkaz do prvního příkazového okna:

```
/opt/mqm/samp/bin/amqspub /FOOTBALL/scores QM2
```

- b. Zadejte tento příkaz do druhého příkazového okna:



### *Klastry publikování/odběru*

Klaster publikování/odběru je standardní klaster produktu IBM WebSphere MQ vzájemně propojených správců front, kde jsou publikace automaticky přesouvány z publikování aplikací do odběrů, které existují v libovolném správci front v klastru.

Klaster, který se používá pro systém zpráv publikování/odběru, se liší od standardního klastru IBM WebSphere MQ. V takovém případě mohou správci front v klastru publikování/odběru existovat na fyzicky oddělených počítačích a každý pár správců front je v případě potřeby automaticky připojen v rámci kanálů klastru. Informace o plánování a konfiguraci klastru IBM WebSphere MQ naleznete v tématu [Jak klastry fungují](#).

Klaster publikování/odběru je vytvořen při definování klastrovaného objektu tématu pomocí nastavení atributu **CLUSTER** na téma, které je nakonfigurováno libovolným správcem front v klastru. Definice tématu je rozšířena na všechny členy klastru. Můžete publikovat a přihlásit se k odběru tématu a libovolný řetězec tématu pod ním ve stromu témat v libovolném správci front v klastru. Publikování se automaticky šíří na odběratele připojené k ostatním správcům front v klastru.

Neklastrovaná aktivita publikování/odběru se může také provádět v klastru publikování/odběru, a to pomocí práce s řetězci témat, které nespádají pod klastrovaný objekt tématu. Toto uspořádání se liší od hierarchie publikování/odběru, v níž jsou všechny odběry šířeny v rámci celé hierarchie. V obou případech je k dispozici podrobnější řízení s použitím rozsahu odběru a publikování.

Použití klastrů v topologii publikování/odběru poskytuje následující výhody:

- Zprávy určené pro odběr u konkrétního správce front ve stejném klastru jsou transportovány přímo do tohoto správce front a není nutné předávat intermediačního správce front. Tím se zlepší výkon a optimalizuje provoz pro publikování/odběr mezi správcem front, ve srovnání s hierarchickou topologií.
- Protože jsou všichni správci front k sobě navzájem přímo připojeni, v této topologii neexistuje jediný bod selhání. Není-li k dispozici jeden správce front, budou odběry ostatních správců front v klastru i nadále moci přijímat zprávy od vydavatelů k dostupným správcům front.
- V systému, který obsahuje více samostatných klastrů, například pokud jsou klastry geograficky rozptýlené, je možné připojit klastry do hierarchie klastrů. Toto připojení je vytvořeno spojením jednoho správce front v každém klastru, aby bylo možné povolit tok publikací a odběrů prostřednictvím sítě; viz [“Kombinování prostorů tématu s více klastry”](#) na stránce 95. Můžete také řídit tok publikací z jednoho klastru do jiného; viz [“Kombinování a izolování prostorů témat ve více klastrech”](#) na stránce 97.

- Aplikace odběru se může připojit k nejbližšímu správci front, a zlepšit tak svůj vlastní výkon. Správce front obdrží všechny zprávy odpovídající registraci odběru klienta od všech správců front v rámci klastru.

Výkon aplikace klienta se také zlepší pro ostatní služby, které jsou požadovány od tohoto správce front. Klientská aplikace může používat jak publikování/odběr, tak systém zpráv typu point-to-point.

- Počet klientů a odběrů pro jednotlivé správce front lze snížit přidáním dalších správců front do klastru pro sdílení pracovní zátěže. Publikace budou automaticky distribuovány klientům v nových správcích front. U některých vzorků použití může tento proces vysoce přizpůsobitelnou a rozšiřitelnou topologii klastru pro publikování/odběr.

Co je třeba zvážit při použití klastrů při publikování/odběru:

- Všichni správci front v klastru publikování/odběru jsou automaticky informováni o všech ostatních správcích front v klastru. Tento proces se liší pro klaster typu point-to-point, o kterém je známo pouze správci front, kteří mají zájem o správce front.
- Správci front v klastru publikování/odběru, které jsou hostiteli jednoho nebo více odběrů v klastrovaném tématu, automaticky vytvářejí odesílací kanály klastru pro všechny ostatní správce front v daném klastru. Správci front také odesílají informace o odběrech každému z nich, i když přijímající správci front nepublikují zprávy v žádných klastrovaných tématech.
- První odběr ze správce front do řetězce tématu pod klastrovaným tématem vede k odeslání zprávy všem ostatním správcům front v klastru. Podobně i poslední odběr na řetězci tématu, který má být odstraněn,

má za následek také zprávu. Čím více jednotlivých řetězců témat je používáno v rámci klastrovaného tématu, dochází k další komunikaci mezi správci front.



#### **POZOR:**

Z důvodů uvedených výše v tomto tématu může zavedení klastrovaného tématu do velkého klastru produktu IBM WebSphere MQ (tj. klastru, který obsahuje mnoho správců front) okamžitě vést k dalšímu načtení každého správce front v klastru a v některých situacích může dojít ke snížení výkonu. Další informace viz [“Výkon tématu klastru”](#) na stránce 72.

Zavedení systému publikování/odběru do klastru správců front, zejména existujícího klastru, je třeba pečlivě naplánovat tak, aby vyhovovalo tomuto snížení výkonu.

Je-li známo, že se klastr nemůže přizpůsobit snížení výkonu publish/odběru, je možné zakázat funkce klastrovaných publikování/odběru ve správcích front pomocí parametru **PSCLUS**. Parametr **PSCLUS** je primárně určen k zastavení závažných problémů, ke kterým může dojít při vytváření klastru publikování/odběru náhodně nebo nesprávně definováním klastrovaného tématu. Další informace o zakázání této funkčnosti viz [“Blokování klastrovaných publikování/odběru v klastru”](#) na stránce 71.

#### *Klastrování publikování/odběru: Nejlepší postupy*

Toto téma obsahuje pokyny pro plánování a administraci klastrů publikování a odběru IBM WebSphere MQ. Informace jsou založené na testování a zpětné vazbě od zákazníků.

Následující informace předpokládají, že uživatel má základní znalosti o klastrech IBM WebSphere MQ, Publikování/odběr a je obeznámen s tématy v produktu [“Distribuované publikování/odběr”](#) na stránce 48. Tyto informace nejsou zamýšleno jako "jedna velikost pro všechny" řešení, ale snaží se sdílet společné přístupy ke společným problémům.

## **Klastry publikování/odběru**

V případě klastru máte v případě potřeby přímé spojení mezi správci front v klastru. Je-li použit klastr pro systém zpráv typu point-to-point, každý správce front v klastru zná pouze informace o dalších klastrových prostředcích, jako jsou ostatní správci front v klastru a v klastrovaných frontách, když se k nim aplikace připojují pomocí požadavku na jejich použití; to znamená, že pracují na potřebách-to-know-to-know-to-know-to-to-know-to-know-to-

Klastr typu publikování/odběr je klastr správců front s obvyklými definicemi kanálů [CLUSDR](#) a [CLUSRCVR](#). Klastr publikování/odběru však také obsahuje alespoň jeden objekt [TOPIC](#) definovaný na alespoň jednom správci front v klastru, ve kterém objekt tématu identifikoval název klastru.

Je-li v klastru definován objekt tématu, může aplikace, která je připojena k jednomu správci front v klastru, odebírat toto téma nebo kterýkoli uzel ve stromu témat pod tímto tématem a přijímat publikování z jiných správců front v daném klastru. Tento proces je dosahováno vytvořením proxy odběrů na všech ostatních správcích front v klastru identifikujících správce front, ve kterém existuje odběr. Takže, když se publikování na dané téma děje ve správci front, ví, že je předá ostatním příslušným členům klastru a že jej doručí k jednotlivým odběrům aplikace.

Aby bylo možné tohoto doručení dosáhnout, musí každý správce front v klastru znát identitu každého dalšího správce front v klastru, jakmile je téma přidáno do klastru. Tato znalost je šířena prostřednictvím správců front úplného úložiště klastru. Publikované zprávy v jednom správci front jsou odesílány pouze jiným správcům front v klastru, o nichž je známo, že mají hostitelské odběry ke stejnému tématu. Chcete-li tohoto procesu dosáhnout, pokud aplikace vytvoří odběr tématu, které je klastrované, musí správce front komunikovat přímo s každým jiným správcem front v klastru prostřednictvím odesílacích kanálů klastru, aby rozšířili proxy odběry.

Tento proces se značně liší od omezené potřeby komunikace a konektivity, která je potřebná, když používáte klastr pro dvoubodové doručení. Požadavky na klastr publikování/odběru se proto liší od požadavků na klastru typu point-to-point (jeden bez klastrovaných témat).

Použití klastrovaných témat rozšiřuje doménu publikování/odběru mezi správci front jednoduchou, ale může vést k problémům, pokud se mechanici a implikace nerozumějí a jsou zvažovány s ohledem na

klastr používaný pro publikování/odběr. Následující doporučené postupy jsou navrženy tak, aby vám pomohly při tomto pochopení a přípravě.

Souhrnnost výkonu klastrovaných publikování/odběru může být v souhrnu škodlivá pro velký klastr a má být pečlivě uváženo a pochopena před jakýmkoli pokusem o použití publikování/odběru v existujícím klastru. Například i jednoduché vytvoření objektu klastrovaného tématu. Může být lepší začít s malým novým klastrem vyhrazeným pro aktivitu publikování/odběru a zvětšování klastru z této oblasti.

## Návrh topologie publikování/odběru

Jak již bylo popsáno výše, při použití publikování/odběru v klastru používáte informace o kapacitě a výkonu. Proto je nejlepší pečlivě zvážit potřebu publikování/odběru pro správce front a omezit ji pouze na počet správců front, kteří ji vyžadují. Po určení minimální sady správců front, kteří potřebují publikovat a odebrat sadu témat, mohou být členy klastru, který obsahuje pouze tyto členy, a žádný jiný správce front.

Zvláště to platí v zavedeném klastru, který již funguje dobře pro systém zpráv typu point-to-point. Z tohoto důvodu platí, že když přecházíte z existujícího velkého klastru do klastru publikování/odběru, je vhodnější vytvořit samostatný klastr pro práci publikování/odběru, kde je možné se pokusit o použití aktuálního klastru, místo použití existujícího klastru. Je možné pokračovat v používání existujících správců front, kteří jsou již v jednom nebo více klastrech mezi dvěma body, je třeba vytvořit podmnožinu těchto správců front členům nového klastru publikování/odběru. Tento nový klastr však musí mít samostatné správců front, kteří jsou konfigurováni jako úplná úložiště, aby bylo možné oddělit další zatížení od existujících úplných úložišť klastru.

Pokud určujete, že klastr nemá být použit pro publikování/odběr v důsledku jeho velikosti nebo aktuálního načtení, je dobrým zvykem zabránit tomu, aby se tento klastr nečekaně dostal do klastru publikování/odběru prostřednictvím jednoduchého vytvoření klastrovaného tématu na libovolném správci front v klastru. Použijte vlastnost správce front produktu **PSCLUS** k dosažení tohoto návrhu, podrobnosti viz téma [Inhibiting clustered publish/subscribe in a cluster](#).

Je také důležité pečlivě zvolit, která témata mají být přidána do klastru: Čím vyšší je tato témata stromu témat, tím více se stávají. Z tohoto důvodu se nedoporučuje umístit kořenové uzly tématu do klastru, aniž byste uvažovali o chování, které je patrné. Je-li to možné, musí být globální témata zřejmá, například pomocí kvalifikátoru vyšší úrovně v řetězci tématu: `/global` nebo `/cluster`.

## Jak velikosti systémů

Klustry publikování/odběru vyžadují mnoho kanálů, protože model se liší od systému zpráv typu point-to-point: Je třeba, aby každý správce front hovořil se všemi ostatními správci front v daném klastru. Model dvoubodového spojení je 'opt in', ale klustry pro publikování/odběr mají nerozlišující charakter s rozjímkou odběru. Proto musí mít správce front úplného úložiště a každý správce front, který je hostitelem lokálních odběrů v klastru publikování/odběru, kapacitu k vytvoření kanálů pro každého člena klastru současně.

Je nejlepší zajistit, aby každý správce front v klastru publikování/odběru dosáhl této kapacity, ale je potvrzeno, že správci front, kteří jsou známí nikdy hostiteli odběrů, nemusí vytvářet kanály s každým jiným správcem front, a proto tuto úroveň kapacity nevyžadují.

Je však třeba dbát na to, aby byl náhodný odběr vytvořený na takovém správci front nebo jakýkoli pokus o ruční resynchronizaci takového správce front s ostatními uživateli v klastru, výsledky ve všech kanálech, které byly spuštěny souběžně. Další informace viz ["Resynchronizace proxy odběrů"](#) na stránce 68.

Klastrované publikování/odběr umožňuje doručení publikovaných zpráv na jednoho správce front k odběrům v jiných správcích front. Ale jako pro dvoubodový systém zpráv může být nákladovost přenosu zpráv mezi správci front škodlivá pro výkon. Proto musí být proveden pokus o vytvoření odběrů pro témata ve stejných správcích front, jako jsou zprávy, které jsou publikovány.

Další úvaha se týká vlivu na výkon systému šíření proxy odběrů. Obvykle správce front odešle zprávu o odběru serveru proxy všem ostatním správcům front v klastru při vytvoření prvního odběru specifického řetězce tématu klastru (není pouze konfigurovaný objekt tématu). Pokud se řešení typu publikování-odběr skládá z mnoha jedinečných řetězců témat, které jsou přihlášeny k odběru, nebo jsou často odebrány a odebrány z odběru, může být mezi všemi správci front v klastru vygenerováno významné

množství odběru proxy odběrů, které negativně ovlivní celkový výkon systému. Chcete-li získat informace o způsobech snížení režie odběru proxy, prohlédněte si příručku [“Výkon tématu klastru”](#) na stránce 72 .

## Resynchronizace proxy odběrů

Za normálních okolností správci front automaticky zajistí, aby proxy odběry v systému správně odrážely odběry jednotlivých správců front v daném klastru.

V případě potřeby však můžete ručně znovu synchronizovat lokální odběry správce front s proxy odběry, které jsou šířeny v rámci klastru, pomocí příkazu `REFRESH QMGR TYPE (PROXYSUB)` .

**Poznámka:** Resynchronizace dočasně vytvoří na klastru náhlé další zatížení odběrů proxy, které pochází ze správce front, kde byl příkaz zadán. Z tohoto důvodu ji nepoužívejte, pokud k tomu nebudete instruovat IBM WebSphere MQ service, IBM WebSphere MQ documentation, or error logging instruing you to do so.

Příklad, kdy se požaduje resynchronizace, je situace, kdy správce front nemůže správně šířit proxy odběry, například proto, že kanál byl zastaven a všechny zprávy nelze zařadit do fronty pro přenos, nebo protože chyba operátora způsobila, že zprávy byly nesprávně odstraněny z fronty `SYSTEM. CLUSTER. TRANSMIT. QUEUE` . V této situaci nejprve opravte původní problém (například restartováním kanálu) a poté zadejte příkaz **REFRESH QMGR TYPE (PROXYSUB)** ve správci front. Všimněte si, že publikace, které byly vynechány kvůli tomu, že proxy odběry nejsou na místě, nejsou obnoveny pro ovlivněné odběry. Tuto nevýhodu je třeba vzít v úvahu.

Resynchronizace vyžaduje, aby správce front spustil kanály pro všechny ostatní správce front v klastru. Správce front, kterého aktualizujete, proto musí mít k dispozici dostatek možností pro komunikaci s každým dalším správcem front v klastru.

### *Témata klastru*

Témata klastru jsou administrativní témata s definovaným atributem **cluster**. Informace o tématech klastru jsou předána všem členům klastru a v kombinaci s lokálními tématy mohou vytvořit v každém správci front jiný prostor témat.

Když definujete na správci front téma klastru, odešle se definice tématu klastru do správců front úplného úložiště. Úplná úložiště následně šíří definici tématu klastru na všechny správce front v klastru, čímž zpřístupní toto téma klastru vydavatelům i odběratelům ve všech správcích front klastru. Správci front, na kterém jste vytvořili téma klastru, se říká hostitel tématu klastru. Téma klastru může být používáno libovolným správcem front v klastru, ale všechny změny v tématu klastru musí být provedeny ve správci front, kde je toto téma definováno (hostitel), v němž je změna šířena na všechny členy klastru prostřednictvím úplných úložišť.

V každém správci front je vytvořen jediný obor názvů témat z lokálních definic témat a definic témat klastru, o kterých je informován. Když se aplikace přihlásí k odběru tématu, které se vyřeší na klastrované téma, produkt IBM WebSphere MQ vytvoří proxy odběr a odešle jej přímo ze správce front, ve kterém je vytvořen odběr, všem ostatním členům klastru. Na rozdíl od samotného klastrovaného tématu proxy odběry nepotečou přes správce front úplného úložiště.

Zprávy publikované v rámci tématu jsou zasílány do všech odběrů známých správci front, k němuž je vydavatel připojen. Jsou-li některé z těchto odběrů proxy odběry, odešle se kopie publikované zprávy správci front, ze kterého pochází proxy odběr. Přijímající správce front poté odešle kopii zprávy do všech lokálních odběrů. Tento proces zajišťuje, že odběratel do klastrovaného tématu přijímá publikování od vydavatelů připojených k libovolnému správci front v klastru a že je do klastru šířen pouze minimální počet publikovaných zpráv.

Máte-li klastrované téma a lokální objekt tématu, bude mít přednost lokální téma. Další informace viz [“Více definic témat klastru”](#) na stránce 70.

Další informace o příkazech, které se mají použít k zobrazení témat klastru, najdete v následujících souvisejících odkazech:

## odběry zástupných znaků

Odběry proxy se vytvářejí při vytváření lokálních odběrů v řetězci tématu, který je interpretováno jako klastrovaný objekt tématu nebo nižší, než je objekt tématu. Je-li odběr pomocí zástupného znaku vyšší v hierarchii témat než kterýkoli z témat klastru, nemá proxy odběry odeslané kolem klastru pro odpovídající téma klastru, a proto neobdrží žádné publikace od jiných členů klastru. Tento příkaz však přijímá publikování z lokálního správce front.

Pokud se však jiná aplikace přihlašuje k odběru řetězce tématu, který se vyřeší nebo pod tématem klastru, proxy odběry jsou generovány a publikace jsou šířeny do tohoto správce front. Při příchodu originálu je vyšší odběr zástupného znaku považován za oprávněného příjemce těchto publikací a obdrží kopii.

Toto chování se liší od lokálně publikovaných zpráv ve stejných tématech. Pokud toto chování není vyžadováno, nastavení **WILDCARD (BLOCK)** na klastrované téma způsobí, že původní zástupný znak nebude považován za legitimní odběr a nebude přijímat žádné publikace (lokální ani odjinud v klastru) na téma klastru nebo jeho dílčí témata.

### Související pojmy

[Práce s administrativními tématy](#)

[Práce s odběry](#)

### Související odkazy

[ZOBRAZIT TÉMA](#)

[ZOBRAZIT STAV TPSTATUS](#)

[ZOBRAZIT POD](#)

### *Atributy tématu klastru*

K návrhu a administraci klastrů publikování a odběru je zapotřebí dobré znalosti atributů témat klastru.

Objekt tématu má řadu atributů, které se týkají topologií publikování/odběru pro více správců front. Když používáte klastr IBM WebSphere MQ k vytvoření takové topologie, tyto atributy mají následující chování.

### PROXYSUB

- **PROXYSUB** je atribut, který řídí, kdy se provádí proxy odběry. Podrobnosti o tom, proč byste mohli chtít změnit tento atribut z výchozí hodnoty **FIRSTUSE**, viz [“Více o mechanismech směrování”](#) na stránce 52.
- Stejně jako u jiných atributů klastrovaného tématu je atribut **PROXYSUB** rozšířen na každého správce front v klastru, nikoli pouze na správce front, na kterém bylo téma definováno. Výsledkem je okamžité výsledky v každém správci front v klastru vytvářejícího zástupný odběr se zástupnými znaky pro všechny ostatní správce front. Výsledkem tohoto procesu je to, že každý správce front vytvoří odesílací kanály klastru pro všechny ostatní správce front a všechny publikované zprávy budou odeslány do každého správce front.

### PURPOSE a SUBSCOPE

**PUBSCOPE** a **SUBSCOPE** určují, zda tento správce front šíří publikace do správců front v topologii (klastr/odběr klastru nebo hierarchie), nebo omezuje rozsah pouze na lokálního správce front. Ekvivalentní úlohu můžete provést programově pomocí příkazu **MQPMO\_SCOPE\_QMGR/MQSO\_COPE\_QMGR**.

- **PUBSCOPE** Je-li objekt tématu klastru definován s produktem **PUBSCOPE (QMGR)**, definice je sdílena s klastrem, ale rozsah publikací, které jsou založené na daném tématu, je pouze lokální a neodesílá se ostatním správcům front v klastru.
- **SUBSCOPE** Je-li objekt tématu klastru definován s produktem **SUBSCOPE (QMGR)**, je definice sdílena s klastrem, ale rozsah odběrů, které jsou založeny na daném tématu, je pouze lokální, proto nejsou do jiných správců front v klastru odeslány žádné proxy odběry.

Tyto dva atributy se společně používají k izolování správce front v součinnosti s ostatními členy klastru na konkrétních tématech. Správce front nepublikuje nebo přijímá publikace z těchto témat a z jiných členů klastru. Tato situace nebrání publikování nebo odběru, pokud jsou objekty tématu definovány v dílčích tématech.



Nastavení parametru **SUBSCOPE** na hodnotu QMGR v lokální definici tématu nezabrání ostatním správcům front v klastru šíření jejich odběrů proxy do správce front, pokud používají klastrovanou verzi daného tématu, s produktem **SUBSCOPE (ALL)**. Pokud však lokální definice rovněž nastaví produkt **PUBSCOPE** na hodnotu QMGR, nebudou tyto odběry proxy odeslány z tohoto správce front.

#### *Více definic témat klastru*

Lokální definice tématu přepíše vzdálenou definici tématu klastru se stejným názvem. Vytvoření více definic jednoho tématu klastru u různých správců front v klastru je také možné. Oba tyto scénáře vyžadují jistou opatrnost, avšak důvody jsou vysvětleny v tomto tématu.

Stejně jako u klastrovaných front, které mají více definic stejného objektu tématu klastru v klastru, zavádí možnost různých vlastností definovaných pro každou z nich. Není jednoduché určit, která verze definice tématu je u každého správce front v klastru patrná, a proto je obtížné určit očekávané chování.

Pokud existují dvě nebo více definic témat klastru pro jeden řetězec tématu, mají různé atributy nebo existují ve více než jednom klastru, zprávy ([AMQ5465](#) & [AMQ5466](#)) jsou zapsány do protokolu chyb a použije se poslední přijatá definice tématu klastru.

Správce front hostitele tématu klastru nesmí odstranit definici tématu a zůstane v klastru, aby se zajistilo, že všechny členy klastru budou nadále známy klastrované téma. Není nezbytně nutné, aby byl tento správce front hostitele neustále dostupný, protože definice tématu klastru je uložena do mezipaměti správci front úplného úložiště a všemi ostatními správci front v jejich dílčích úložištích klastru. Toto využití mezipaměti umožňuje nejméně 60 dnů dostupnosti tématu při nedostupnosti správce fronty hostitele. Další informace o tomto tématu viz [“Klíčové role pro správce front klastru pro publikování/odběr”](#) na stránce 75.

## **Lokální potlačení definice tématu klastru**

Může být nezbytné potlačit chování klastrovaného tématu u určitých správců front v klastru. Toto potlačení lze dosáhnout definováním lokálního objektu tématu a přepsat objekt tématu klastru se stejným řetězcem tématu a použít jej k publikování pouze lokálně připojeným odběratelům.

Dokonce i když je vytvořena lokální definice tématu pro potlačení klastrovaného tématu ve správci front, bude správce front nadále přijímat proxy odběry od ostatních členů klastru za použití definice klastrovaného tématu. Ve výchozím nastavení jsou zprávy publikované lokálně i nadále odesílány do vzdálených správců front, aby bylo možné přijmout proxy odběry. Není-li tato úprava vyžadována, zadejte v lokálním objektu tématu **PUBSCOPE** (QMGR) a zajistěte, aby aplikace vydavatele připojené k tomuto správci front byly publikovány pouze pro lokální odběratele.

## **Úprava definice tématu klastru**

Potřebujete-li upravit definici tématu klastru, upravte ji ve stejném správci front, na kterém byl definován, hostitel tématu klastru. Nevytvářejte definici stejného tématu klastru v jiném správci front v klastru. Při definování daného tématu znovu dojde ke dvěma hostitelům tématu klastru pro stejné téma klastru.

Při definování tématu klastru vícekrát se vytvoří potenciálně konfliktní definice a možnost, že různí správci front používají různé definice v různých časových okamžicích.

## **Přesun definice tématu klastru do jiného správce front v klastru**

Možná budete muset přesunout definici tématu klastru z jednoho správce front v klastru do jiného, například při vyřazování správce front z klastru z provozu. Chcete-li přesunout definici tématu klastru do jiného správce front v klastru, aniž byste přerušili tok publikací, musíte postupovat podle těchto kroků. Tento příklad přesune definici z QM1 do QM2.

1. Vytvořte duplikát definice tématu klastru v systému QM2 se stejnými atributy jako je definice volby QM1.
2. Počkejte, až nová definice bude šířena v celém klastru správci front úplného úložiště. Šíření lze určit zobrazením tématu klastru u jednotlivých členů klastru pomocí příkazu (**DISPLAY CLUSTER**) a kontrolou definice pocházející z produktu QM2.
3. Odstraňte definici tématu klastru z produktu QM1.

Po odstranění původní definice z QM1 je možné upravit definici v QM2 , pokud je to požadováno, aniž by došlo ke konfliktu ve vlastnostech.

## Nahrazení definice tématu klastru ve správci front se selháním

V předchozím scénáři nemusí být možné odstranit definici z QM1 , pokud QM1 není k dispozici po dobu. V tomto scénáři je přijatelné pracovat jak s definicemi, tak i s existencí.

Pokud se pak stane požadavkem na úpravu definice klastrovaného tématu, je možné upravit verzi na QM2 ve znalostech, že definice QM2 je novější než definice QM1 , a tudíž má převahu. Během tohoto období se však chyby zapíší do protokolů chyb správců front, protože existuje konfliktní definice tématu klastru. Odstraňte chybu co nejdříve odebráním duplicitní definice tématu klastru z produktu QM1 , až bude možné ji restartovat.

Případně, pokud se QM1 nikdy nevrátí do klastru (například neočekávané vyřazení z provozu po katastrofálním hardwarovém selhání), lze příkaz `RESET CLUSTER` použít k vynucené vysunutí správce front. Příkaz **RESET CLUSTER** automaticky odstraní všechny objekty témat, které jsou hostovány v cílovém správci front.

### *Blokování klastrovaných publikování/odběru v klastru*

Zavedení systému publikování/odběru do klastru správců front, zejména existujícího klastru, musí být pečlivě naplánováno tak, aby vyhovovalo jakémukoli snížení výkonu.

Zavedení klastrovaného tématu do velkého klastru IBM WebSphere MQ (jeden obsahující mnoho správců front) může okamžitě vést k dalšímu načtení každého správce front v klastru, a v některých situacích také snížení výkonu. Proto je třeba pečlivě plánovat zavedení publikování/odběru. Další informace viz [“Výkon tématu klastru”](#) na stránce 72.

Je-li známo, že klastr nemohl pojmout režijní náklady na publikování/odběr, je možné zakázat funkce klastrovaných publikování/odběru ve správci front nastavením atributu správce front **PSCLUS** na hodnotu `DISABLED`.

Nastavení parametru **PSCLUS** na hodnotu `DISABLED` upravuje tři aspekty funkcí správce front:

- Administrátor tohoto správce front již není schopen definovat objekt tématu jako klastrovaný.
- Příchozí definice témat nebo proxy odběry z jiných správců front jsou odmítnuty (je protokolována varovná zpráva, která informuje administrátora o nesprávné konfiguraci).
- Úplná úložiště již nesdílejí informace o každém správci front se všemi ostatními částečnými úložišti automaticky, když obdrží definici tématu.

Ačkoli **PSCLUS** je parametrem každého jednotlivého správce front v klastru, není zamýšlen selektivně zakázat publikování/odběr v podmnožině správců front v klastru. Kromě čehokoli jiného by tato metoda měla za následek časté chybové zprávy, které by byly považovány za proxy odběry a definice témat byly vždy považovány za zamítnuté a odmítnuté. V ideálním případě při použití této volby trvale nastavte všechny správce front v klastru tak, aby byly zakázány. Pokud se správce front podílí na jednom nebo více klastrech nebo klastrech publikování/odběru, a také jeden nebo více tradičních klastrů nebo klastrů, musí být na tomto správci front nastaven parametr **PSCLUS** na hodnotu `ENABLED` . Prohlédněte si následující informace o zakázání v úplných úložištích.

Důležité je, že nastavení hodnoty **PSCLUS** na hodnotu `DISABLED` ve všech správci front úplného úložiště v klastru zabrání tomu, aby jakákoli definice klastrovaného tématu byla nesprávně nakonfigurovaným dílčím úložištěm ovlivnila ostatní správce front v klastru. V takových scénářích je nekonzistence uvedena v protokolech chyb správců front úplného úložiště.

Když se překrývá tradiční dvoubodový klastr s klastrem pro publikování odběru, je důležité pro každou z nich použít samostatnou sadu úplných úložišť. Toto uspořádání umožňuje, aby byly definice témat a informace o všech správci front povoleny pouze pro tok v klastru publikování/odběru.

Existují určité upozornění na použití tohoto parametru, které pomáhají předcházet nekonzistentním konfiguracím. Žádné klastrované objekty tématu nemohou existovat v žádném klastru, jehož je tento správce front členem, když upravujete z `ENABLED` na `DISABLED`. Před zakázáním této funkce je třeba vymazat všechna taková témata (dokonce i vzdáleně definovaná)

Další informace o produktu **PSCLUS** naleznete v tématu [ALTER QMGR \(PSCLUS\)](#).

#### *Výkon tématu klastru*

Charakteristiky výkonu témat klastru vyžadují zvláštní pozornost, protože se liší od charakteristik výkonu front klastru, a špatně zvažované použití může potenciálně být zdrojem problémů s výkonem ve velkých nebo nevyvážených klastrech.

### **Omezení vlivu publikování/odběru na výkon**

Ve správci front v klastru existují dva zdroje pracovní zátěže: přímo obsluhují zprávy pro aplikační programy a zpracovávají zprávy a kanály potřebné ke správě klastru. V typickém klastru mezi dvěma body je pracovní zátěž klastrového systému do značné míry omezena na informace, které členové klastru výslovně požadují (viz porovnání v produktu "[Charakteristiky výkonu klastrů publikování/odběru](#)" na stránce 75). Proto v jiných než velmi velkém klastru, například v případě, který obsahuje tisíce správců front, můžete při zvažování výkonu správce front do značné míry snížit vliv na výkon správy klastru.

V klastru publikování/odběru jsou informace, jako jsou klastrovaná témata a proxy odběry, odeslány na všechny členy klastru bez ohledu na to, zda se všichni správci front klastru aktivně účastní publikování/odběru zpráv. Tento proces může v systému vytvořit značné dodatečné zatížení. Proto je třeba brát v úvahu vliv správy klastru na výkon správce front, a to jak při jeho časování, tak i v jeho velikosti.

Chcete-li snížit vliv správy klastru publikování/odběru na výkon klastru, zvažte následující dva návrhy:

1. Proveďte aktualizaci klastru, tématu a odběru aktualizací v době mimo špičku dne.
2. Zvažujete-li přidávání témat k publikování/odběru do existujícího velkého klastru, protože klastr již existuje, zvažte, zda můžete definovat mnohem menší podmnožinu správců front zahrnutých do publikování/odběru a zda se má klastr "překrývat". Tento klastr je pak klastr, kde jsou definována témata klastru. Přestože někteří správci front jsou nyní ve dvou klastrech, je celkový účinek publikování/odběru snížen:
  - a. Velikost klastru publikování/odběru je menší.
  - b. Správci front, kteří nejsou v klastru publikování/odběru, jsou mnohem méně ovlivněni dopadem provozu správy klastru.

### **Vyvažování výrobců a spotřebitelů**

Důležitým konceptem ve výkonu asynchronního systému zpráv je *zůstatek*. Pokud nejsou spotřebitelé zpráv vyvázeni s producenty zpráv, hrozí nebezpečí, že se nahromaděné nespotřebované zprávy mohou nahromadit a vážně ovlivňovat výkon více aplikací.

V topologii systému zpráv typu point-to-point je snadno srozumitelná relace mezi spotřebiteli zpráv a producenty zpráv. Odhady produkce a spotřeby zpráv můžete získat, frontu podle fronty, kanál podle kanálu. Je-li nedostatek rovnováhy, jsou kritická místa snadno identifikována a pak napravena.

Je těžší zjistit, zda jsou vydavatelé a odběratelé vyvázeni v topologii publikování/odběru. Začněte od jednotlivých odběrů, které se přeloží na klastrované téma, a vrátíte se zpět ke správcům front s vydavateli v daném tématu. Vypočítejte počet publikací proudících na každého odběratele z každého správce front.

Každá publikování, která odpovídá odběru ve vzdáleném správci front v klastru (na základě proxy odběrů), je vložena do produktu `SYSTEM . CLUSTER . TRANSMIT . QUEUE`. Pokud má více vzdálených správců front pro tuto publikaci proxy odběry, více kopií zprávy se umístí do přenosové fronty, která je cílená pro různé odesílací kanály klastru.

Tyto publikace jsou zaměřeny na frontu `SYSTEM . INTER . QMGR . PUBLS` ve vzdálených správcích front. Každý správce front zpracovává zprávy přicházející do této fronty a doručují je do správných odběrů v daném správci front.

Z tohoto důvodu monitorujte zatížení v následujících bodech, kde mohou nastat kritická místa:

- Samotné jednotlivé fronty odběru:
  - Toto kritické místo by znamenalo, že odebírající aplikace nebude publikování přijímat tak rychle, jak jsou zveřejňována.



- Fronta SYSTEM . INTER . QMGR . PUBS :
  - Správce front přijímá publikace od jednoho nebo více vzdálených správců front rychleji, než je může distribuovat do lokálních odběrů.
- Klastrové kanály mezi správcem fronty publikování, správci front odběru a převodovými frontami klastru (standardně SYSTEM . CLUSTER . TRANSMIT . QUEUE ) ve správci front publikování:
  - Buď jeden nebo více kanálů klastru není spuštěno, nebo jsou zprávy publikovány do lokálního správce front rychleji, než je kanál může doručit do vzdáleného správce front.
- Pokud publikační aplikace používá rozhraní publikování/odběru ve frontě, fronta SYSTEM . BROKER . DEFAULT . STREAM a všechny ostatní fronty proudu vypsané ve frontě SYSTEM . QPUBSUB . QUEUE . NAMELIST a fronty SYSTEM . BROKER . DEFAULT . SUBPOINT a všechny ostatní fronty podbodů, jak je uvedeno v publikaci SYSTEM . QPUBSUB . SUBPOINT . NAMELIST, je třeba také zvážit:
  - Zprávy jsou aplikacemi lokální publikující rychleji, než může lokální správce front zpracovat zprávy.

## Aspekty výkonu odběru

Jak již bylo popsáno výše, je-li na správci front nastaven odběr pro řetězec tématu, který se vyřeší na klastrované téma, musí správce front zajistit, aby každý jiný správce front v klastru měl pro dané téma nastaven odběr serveru proxy. K dosažení tohoto výsledku správce front vytvoří a odešle zprávu o odběru proxy všem ostatním správcům front v klastru.

Výsledkem použití výchozí konfigurace je pouze to, že vytvoření odběru v klastrovaném tématu nemá za následek odeslání nových odběrů proxy, pokud již existuje odběr lokálního správce front na přesně stejný řetězec tématu. V této situaci nejsou vyžadovány žádné další proxy odběry, protože přijíždějící publikace jsou doručeny všem odpovídajícím odběrům, nikoli pouze původním odběru pro řetězec tématu.

Alternativou k výchozí konfiguraci viz [“Zakázání jednotlivých odběrů proxy”](#) na stránce 74.

Selektory odběru nejsou vzaty v úvahu, takže dva odběry stejného řetězce tématu, ale s různými selektory, stále sdílejí odběry proxy. Tato situace může také znamenat, že publikace, které odpovídají řetězci tématu, jsou šířeny do správce front odběratele, a to i v případě, že se publikování neshoduje s voličem odběru.

Po odstranění posledního odběru řetězce tématu ze správce front bude vytvořena a odeslána všem správcům front ekvivalentní zpráva o zprávě odběru serveru proxy. Tento proces odebere proxy odběry ze vzdálených správců front.

Z těchto důvodů může velikost klastru a frekvence odběrů pro různé řetězce témat výrazně zatěžovat samotný klastr a při plánování klastru a témat, která mají být použita aplikacemi publikování/odběru, je třeba brát v úvahu.

Při zvažování zatížení systému z přenosu proxy odběru monitorování kromě monitorování front uvedených v části [“Vyvažování výrobců a spotřebitelů”](#) na stránce 72 bude monitorovat následující fronty.

- SYSTEM.INTER.QMGR.FANREQ ve správci front odběratele.
- SYSTEM.INTER.QMGR.CONTROL ve všech ostatních správcích front v klastru.

Jakýkoliv významný počet nevyřízených zpráv v těchto frontách znamená, že změna rychlosti odběru je příliš velká pro daný systém nebo správce front není v klastru správně funkční. Buď má být zakázána podpora publikování/odběru (viz **PSMODE** v části ALTER QMGR) nebo se vyskytl problém, který vyžaduje další zkoumání. V tomto bodě zkontrolujte protokoly chyb správce front.

## Omezení přenosu proxy odběru

Je-li rezie na proxy odběr vysoká, je třeba provést kroky ke snížení tohoto stavu. To může být možné prostřednictvím konsolidace obecného tématu nebo změnou na model vysílání pro publikace mezi správci front.

Jedná se o obecné doporučení pro publikování/odběr, které vyhodnocuje použití řetězců témat s cílem zjistit, zda je možné je konsolidovat způsobem, jak snížit celkové zatížení prostředků systému. Použití

mnoha odlišných, dočasných řetězců témat představuje určitou úroveň režie správy u každého správce front v systému, kde jsou připojeny vydavatele nebo odběry. Snižování počtu a přechodné povahy řetězců témat, a tedy vydavatelé a odběry, snižuje dopad na systém.

Jednou metodou pro omezení přenosů odběru proxy je vyhledání odběrů pro stejný řetězec tématu ve stejném správci front. Tato metoda umožňuje tomuto správci front odeslat jeden proxy odběr jiným správcům front namísto toho, aby měl více správců front, kteří odesílají proxy odběry, každý pro svou vlastní sadu odběrů na stejném řetězci tématu. Tento postup také optimalizuje směrování publikací v rámci klastru.

## Zakázání jednotlivých odběrů proxy

V některých situacích, kdy je sada různých řetězců témat přihlášená k odběru v rámci klastru velká a neustále se mění, může být lepší změnit z modelu šíření odběru na model broadcast publikování. Tento upřednostňovaný model je místo, kde je každé publikování na libovolném klastru automaticky odesláno do každého správce front v klastru, bez ohledu na existenci odběrů na daných správcích front.

Přijímající správci front pak mohou doručovat zprávy do lokálních odběrů, které existují, nebo zprávu zahodit. V tomto modelu není třeba vytvářet a odstraňovat jednotlivé odběry proxy založené na existenci odběrů. Při spuštění v tomto režimu je pravděpodobné, že publikovaná zátěž zdrojů zpráv se zvyšuje, protože všechny publikace jsou odeslány všem správcům front. Proto musí mít správci front v klastru kapacitu pro zpracování této dodatečné zátěže.

Povolte model vysílání pomocí následujících kroků konfigurace:

1. Každý správce front, který je hostitelem odběrů, musí být nakonfigurován tak, aby neodesílal proxy odběry, které odpovídají lokálním odběrům klastrovaných témat. Tato konfigurace vyžaduje nastavení následujícího parametru ladění v každém souboru `qm.ini` správce front, a to před definicí témat klastru nebo vytvořením odběrů v klastru:

```
TuningParameters:  
  pscProxySubFlags=1
```

2. Po nastavení parametru ladění musí být všichni správci front restartováni.
3. Po restartování správců front lze definovat klastrované téma či témata. Každé téma klastru musí být nastaveno **PROXYSUB** na **FORCE**.

### Převrácení chování

Chcete-li změnit režim operace popsany dříve v produktu [“Zakázání jednotlivých odběrů proxy”](#) na [stránce 74](#), postupujte takto:

1. Odeberte parametr ladění ze souboru `qm.ini` pro každého správce front.
2. Restartujte všechny správce front.
3. Zadejte příkaz **REFRESH QMGR TYPE (PROXYSUB)** pro každý správce front, který je hostitelem odběrů.
4. Nastavte **PROXYSUB** na **FIRSTUSE** na klastrovaných tématech nebo tématech.



**POZOR:** Pokud nejsou všechny kroky v dokumentovaném pořadí dokončeny v dokumentovaném pořadí, v povolujícím i obrácení tohoto chování nemusí dojít k opravení toku publikování v odběrech.

### Poznámka: Implikace při nastavení parametru **PROXYSUB (FORCE)**

Jak již bylo popsáno výše v tomto tématu, může atribut tématu produktu **PROXYSUB (FORCE)** snížit provoz proxy odběru, ale musí být používán s opatrností. Atribut **PROXYSUB (FORCE)** je šířen do všech správců front v klastru, nikoli pouze správce front, na kterém bylo téma definováno. Výsledkem je okamžité výsledky v každém správci front v klastru vytvářejícího zástupný odběr se zástupnými znaky pro všechny ostatní správce front. Výsledkem tohoto procesu je, že každý správce front vytvoří odesílací kanály klastru pro všechny ostatní správce front a všechny publikované zprávy budou odeslány do každého správce front.

Nastavení této vlastnosti ve velkém nebo zaneprázdněném klastru může mít za následek další zatížení systémových prostředků.

## Charakteristiky výkonu klastrů publikování/odběru

Je důležité zvážit, jak změnit atributy klastru publikování/odběru, jako např. přidání správce front, tématu nebo odběru do klastru, ovlivní výkon aplikací spuštěných v klastru.

Porovnejte klastr typu point-to-point s klastrem pro publikování/odběr, pokud jde o dvě úlohy správy.

Za prvé, dvoubodový klastr:

1. Je-li definována nová fronta klastru, jsou informace o místu určení předány správci front úplného úložiště a jsou odeslány pouze ostatním členům klastru při prvním odkazu na frontu klastru (například při pokusu o otevření aplikace). Tyto informace jsou následně uloženy do mezipaměti správce front za účelem odebrání potřeby vzdáleného načtení informací při každém přístupu k frontě.
2. Přidání správce front do klastru nemá přímý vliv na načtení v jiných správcích front. Informace o novém správci front jsou odeslány do úplných úložišť, ale kanály nového správce front od jiných správců front v klastru jsou vytvářeny a spuštěny pouze v případě, že provoz začíná proudit do nového správce front nebo z něj.

Stručně řečeno, načtení ve správci front v klastru typu point-to-point se vztahuje k provozu zpráv, které zpracovává pro aplikační programy, a nespojuje přímo s velikostí klastru.

A za druhé klastr pro publikování/odběr:

1. Je-li definováno nové téma klastru, jsou informace předány správcům front úplného úložiště a okamžitě přímo všem členům klastru, což způsobí spuštění kanálů pro každého člena klastru z úplných úložišť, pokud ještě nejsou spuštěny.
2. Je-li odběr vytvořen v tématu klastru na novém řetězci tématu, jsou informace z tohoto správce front odeslány přímo všem ostatním členům daného klastru, což způsobí spuštění kanálů pro každého člena klastru z tohoto správce front, pokud již není spuštěn.
3. Když se nový správce front připojí ke stávajícímu klastru, jsou informace o všech klastrovaných tématech z správců front úložiště odeslány do správce front úplných úložišť. Nový správce front poté synchronizuje informace o všech odběrech témat klastru v klastru se všemi členy klastru, což způsobí vytvoření kanálů a jejich spuštění pro každého člena klastru z nového správce front.

Stručně řečeno, načtení správy klastru u libovolného správce front v klastru roste s počtem správců front, klastrovaných témat a proxy odběrů v rámci klastru, bez ohledu na místní použití těchto témat klastru na každém správci front.

### *Klíčové role pro správce front klastru pro publikování/odběr*

Podobně jako u klastrů typu point-to-point existují dvě klíčové role pro správce front v klastru publikování/odběru, jako správce front úplného úložiště a jako hostitelé témat klastru.

### **Úložiště souborů**

Správce front úplného úložiště má roli pro vkládání definic objektů do jiných členů klastru; v případě klastrů publikování/odběru protlačte definice sdružených témat v klastru na jiné členy klastru.

### **Hostitel tématu klastru**

Hostitel tématu klastru je správce front, ve kterém je definován klastrovaný objekt tématu. V každém správci front v klastru publikování/odběru můžete definovat objekty klastrovaných témat. Objekt tématu klastru je odeslán na správce front úplného úložiště, který poté předání odešle všem ostatním správcům front v klastru, kde je uložen v mezipaměti pro použití vydavateli a odběrateli spuštěnými ve všech správcích front v klastru.

## Dostupnost a správa

Měli byste definovat dvě úplná úložiště v klastru, abyste maximalizovali dostupnost definic témat klastru v klastru.

Pokud jde o klastry systému zpráv ve frontě, v klastrech publikování/odběru, které mají pouze dva vysoce dostupné počítače mezi mnoha počítači, je dobrým zvykem definovat vysoce dostupné počítače jako úplná úložiště.

Ve frontách klastrů můžete zvýšit dostupnost a propustnost fronty klastru tím, že *definujete* stejnou frontu klastru na více správcích front v klastru. Zprávy jsou pak vyrovnány pracovní zátěží mezi nimi. Naproti tomu v klastrech publikování/odběru je klastrované téma *dostupné* na všech správcích front v klastru, ale neprovádí se žádné vyrovnávání pracovní zátěže přenosů publikování/odběru. Místo toho by měly být samostatné odběry a vydavatelé šířeny mezi různými správci front, aby se rozšířilo načtení publikování/odběru. Pokud správce front, na kterém jste definovali téma klastru, přestane být k dispozici, budou ostatní správci front nadále zpracovávat požadavky na publikování/odběr pro dané téma.

Pokud však správce front, ve kterém jste definovali objekt tématu klastru, nebude nikdy znovu zpřístupněn, budou nakonec objekty témat uložené v mezipaměti v ostatních správcích front odstraněny a téma bude nedostupné. Tento proces nastává nejméně po 60 dnech (v závislosti na tom, kdy byla definice tématu naposledy aktualizována), od okamžiku, kdy se definice tématu stala nedostupnou.

Po 60 dnech zotavování správce front, ve kterém jste definovali objekty tématu klastru, je třeba věnovat zvláštní pozornost tomu, aby byl hostitel tématu klastru vysoce dostupný. Lhůta 60 dnů postačuje k zajištění technických problémů; období 60 dnů je pravděpodobně překročeno pouze z důvodu administrativních chyb. Chcete-li tuto možnost zmírnit, pokud hostitel tématu klastru není k dispozici, všichni členové zprávy protokolu chyb zápisu do klastru budou každou hodinu aktualizovat, že objekt tématu klastru uložený v mezipaměti nebyl aktualizován. Na tuto zprávu reagujte a ujistěte se, že je spuštěn správce front, na kterém je definován objekt tématu klastru.

Je možné, že budete moci definovat stejný objekt tématu klastru u ostatních správců front. Každá definice má za následek přesunutí dalšího objektu tématu klastru do ostatních správců front v klastru, včetně ostatních hostitelů témat klastru. Nyní, když se hostitel tématu klastru stane nedostupným pro více než 60 dní, je z ostatních hostitelů odebrán pouze jeho verze objektu tématu klastru. Ostatní verze objektu tématu klastru zůstanou zachovány. Jedná se o požadavek, že všechny definice pro specifické téma v klastru jsou identické, jinak je obtížné zjistit, která definice tématu je používána správcem front. Nejčerstvější kopií na každém hostiteli je vždy objekt tématu klastru, který se používá.

Přidaná ochrana více definic témat klastru proti zvýšené administrativní složitosti: se zvýšenou složitostí přichází s větší pravděpodobností lidské chyby.

Na rozdíl od hostování klastrované fronty není správce front hostitele pro definici klastrovaného tématu žádný další přenos zpráv aplikace. Tento provoz je omezen na správce front, ve kterých jsou vytvořeny odběry a publikované zprávy. Klastrované téma je možné hostovat na správci front, který nedělá ani jeden z nich. Tato situace znamená, že i když to není povinné, je často rozumné hostovat klastrovaná témata pro správce front úplného úložiště pro klastr, protože tito správci front mohou být zajištěni s vyšší úrovní dostupnosti a mají na nich přísnější administrativní kontrolu. Toto uspořádání snižuje možnost nesprávně upravit nebo odstranit definice nebo dokonce i správce front.

#### *Překrývající se podpora klastrů a publish/subscribe*

S klastry IBM WebSphere MQ může být jeden správce front členem více než jednoho klastru. Toto uspořádání je známé jako překrývající se klastry. Klastrovaná témata v klastrech publikování/odběru se chovají odlišně pro fronty, když jsou klastry překlopené ve správci front. Toto chování musí být jasně chápáno, když používáte klastrované publikování/odběr s překrývajícími se klastry.

Na rozdíl od fronty neexistuje schopnost přidružit definici tématu s více než jedním klastrem. Proto je rozsah proxy odběrů vytvořených v klastru omezen na jediný klastr, ve kterém je definováno klastrované téma. Každý správce front má však jeden strom témat, který obsahuje všechna lokální témata a všechna známá klastrovaná témata z libovolného klastru, jehož členem je. Z tohoto důvodu je možné takový systém, kde lze těžko pochopit chování publikování/odběru, architektu.

#### **Integrace více klastrů publikování/odběru**

Pro zprávy typu point-to-point je důvodem pro vytvoření jednoho správce front více než jeden klastr, aby se vytvořila brána klastru mezi dvěma klastry. Další informace o tomto tématu najdete v tématu [Překrývání klastrů](#). Tato brána klastru umožňuje směřovat zprávy typu point-to-point, které pocházejí z jednoho klastru, směřovat na dotazy v jiném klastru. Klastry publikování/odběru dědí schopnost

překrytí z tradičních klastrů správců front. Tento mechanismus však nelze použít pro směřování publikací a odběrů z jednoho klastru do jiného.

Místo toho je třeba pomocí hierarchie publikování/odběru propojit správce front s použitím publikování a odběrů od správců front v jednom klastru do jiného. Toto uspořádání lze dosáhnout explicitním vytvořením hierarchického vztahu nadřazený-podřazený mezi jedním správcem front v jednom klastru s jiným správcem front v jiném klastru. Tato relace umožňuje tok všech proxy odběrů mezi klastry, a tedy všechny odpovídající publikace. Další informace o tomto vztahu viz [“Hierarchie publikování/odběru”](#) na stránce 79.

Způsob omezení toku publikování a odběrů mezi klastry je použití správce front brány, který není v žádném z klastrů, viz [“Kombinování a izolování prostorů témat ve více klastrech”](#) na stránce 97.

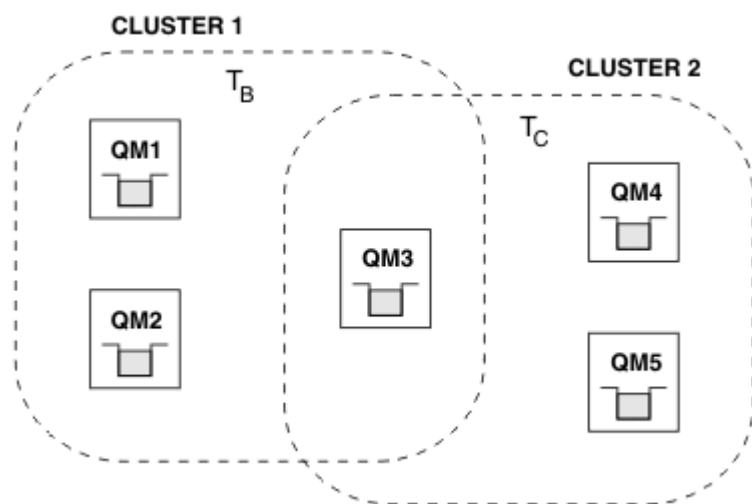
### **Překrývání klastrů, jeden strom témat**

Každý správce front má jeden Strom témat, který obsahuje lokální témata a všechna známá klastrovaná témata. Další zvažování se překrývajícími se dvěma klastry, a to jak pomocí publikování/odběru, je, že je možné, aby správce front v každém klastru definoval klastrované téma se stejným názvem, nebo aby definoval jinak pojmenovaná klastrovaná témata, která mají stejný řetězec tématu. Ve správcích front, kteří jsou členy obou klastrů, vznikají konflikty při informování o více definicích témat klastru, jeden pro každý klastr. Správce front ohlásil problém, ale správce front pokračuje v práci a používá pouze nejnovější definici klastrovaného tématu. Proto se chování stává nedeterministický a nelze je spoléhat.

Z tohoto důvodu musí překrývající se klastry, které používají klastrované publikování/odběr, zvážit jejich obor názvů témat, aby obsáhly všechny klastry, a pojmenujte jejich objekty témat a strukturovat jejich řetězce témat odpovídajícím způsobem. Poté můžete použít správce front v překrytí k publikování a odebírat z obou klastrů předvídatelně.

V [Obrázek 33](#) na stránce 77,  $T_B$  a  $T_C$  jsou definice témat, které se nepřekrývají. Vydavatel připojený k serveru QM3se v klastru překrývá, je schopen publikovat do obou témat ve svých klastrech. Odběratel připojený k produktu QM3 v překryvu se může přihlásit k odběru témat v obou klastrech.

Alternativním způsobem přemýšlení o produktu [Obrázek 33](#) na stránce 77 je zvážit odběry proxy. Aplikace připojená ke správci front QM3se přihlašuje k odběru tématu, které se interpretuje jako objekt tématu  $T_B$  (který existuje pouze v produktu CLUSTER 1), a to pouze v případě, že jsou odběry proxy odesílány ze správce front QM3 pouze na správce front QM1 a QM2. Aplikace připojená ke správci front QM3 se přihlašuje k odběru tématu, které se interpretuje jako objekt tématu  $T_C$  (který existuje pouze v produktu CLUSTER 2). Odběr má za následek odeslání odběrů proxy z správce front QM3 pouze na správce front QM4 a QM5.



*Obrázek 33. Překrývání klastrů: každé přihlášení k odběru různých témat je dva klastry.*

Vydavatelé a odběratelé správců front, kteří se nepřekrývají, mohou publikovat a odebírat pouze témata ve svém klastru, například odběratel řetězce tématu v produktu QM2 nepřijímají zprávy

publikované do stejného řetězce tématu publikovaného z produktu QM5 bez ohledu na to, zda jsou tato témata klastrovaná. K dosažení tohoto uspořádání je vyžadována hierarchie publikování/odběru.

### **Překrývání klastrů, odběry s použitím zástupných znaků**

Z důvodů uvedených v předchozí části tohoto tématu je třeba při přihlášení k odběru témat ve správci front, který je členem více klastrů, používat zástupné znaky.

V předchozím příkladu předpokládejme, že tyto dva objekty témat byly nakonfigurovány jako:

- T<sub>B</sub>: Název tématu 'Football', řetězec tématu 'CLUSTER1'. klastru '/Sport/Football'
- T<sub>C</sub>: Název tématu 'Tennis', řetězec tématu 'CLUSTER2'. klastru '/Sport/Tennis'

V tomto scénáři jsou dvě klastrovaná témata jasně oddělena, přičemž se nepřekrývají ani v názvu tématu, ani v řetězci tématu.

Aplikace připojená k produktu QM3 může vytvořit odběr produktu '/Sport/Football' a odběr produktu '/Sport/Tennis'. Pak budou přijímat jakékoli publikace z těchto dvou klastrů. Nicméně, jak je popsáno v části "Objekty administrativního tématu" na stránce 35, pokud se mají přihlásit k odběru '/Sport/#', s úmyslem přijímat publikace jak na '/Sport/Football', tak na '/Sport/Tennis', tento model není rozpoznán jako klastrované téma v žádném z klastrů, a proto nebudou vytvořeny žádné proxy odběry. Pak budou chybět publikace od jiných správců front v obou klastrech.

Jak již bylo popsáno, není platné vytvořit klastrované téma pro '/Sport/#' v obou CLUSTER 1 a CLUSTER 2, protože tato klastrovaná témata by byla konfliktní a informativní zprávy jsou zapsány do protokolů chyb, aby to označovaly. Avšak je to 'povoleno' vytvořit takové téma v jednom z klastrů, řekněme CLUSTER 1. Now a subscription to '/Sport/#' in QM3 would result in proxy subscriptions being sent to the queue managers in CLUSTER 1 only, so still, publications to '/Sport/Tennis' from QM4 or QM5 would still fail to be received.

Jediným řešením v tomto scénáři je pokračovat ve vytváření dvou samostatných odběrů.

### *Aspekty REFRESH CLUSTER pro klastry publikování/odběru*

Vydáním příkazu **REFRESH CLUSTER** se ve správci front dočasně zruší lokální zadržení informací o klastru, včetně všech témat klastru a jejich přidružených proxy odběrů.

Doba potřebná k zadání příkazu **REFRESH CLUSTER** do bodu, kdy správce front znovu získá úplné informace o nezbytných informacích týkajících se klastrovaných publikování/odběru, závisí na velikosti klastru, dostupnosti a reakční schopnosti správců front úplného úložiště.

Během zpracování aktualizace dochází k přerušení provozu typu publikování/odběru v klastru publikování/odběru. Pro velké klastry může použití příkazu **REFRESH CLUSTER** v průběhu zpracování způsobit narušení klastru a poté znovu ve 27. denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zúčastněným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost. Z těchto důvodů musí být příkaz **REFRESH CLUSTER** použit v klastru publikování/odběru pouze tehdy, když se pod vedením vašeho centra podpory IBM.

Narušení klastru se může objevit zvnějšku jako tyto symptomy:

- Odběry témat klastru v tomto správci front nepřijímají publikování od vydavatelů, kteří jsou připojeni k jiným správcům front v klastru.
- Zprávy publikované v rámci témat klastru v tomto správci front nejsou šířeny do odběrů u jiných správců front.
- Odběry témat klastru na tomto správci front vytvořené během tohoto období nekonzistentně odesílají proxy odběry do jiných členů klastru.
- Odběry témat klastru na tomto správci front, které byly odstraněny během tohoto období, nejsou konzistentně odebírající proxy odběry z jiných členů klastru.
- 10-sekundové pauzy, nebo delší, při doručování zpráv.
- Selhání produktu **MQPUT**, například MQRC\_PUBLICATION\_FAILURE.
- Publikace umístěné ve frontě nedoručených zpráv s příčinou MQRC\_UNKNOWN\_REMOTE\_Q\_MGR

Z těchto důvodů je třeba, aby aplikace publikování/odběru byly uvedeny do klidového stavu před zadáním příkazu **REFRESH CLUSTER**.

Viz také [Poznámky k použití pro REFRESH CLUSTER a Klastrování: Použití doporučených postupů REFRESH CLUSTER](#).

Po zadání příkazu **REFRESH CLUSTER** pro správce front v klastru pro publikování/odběr počkejte, dokud nebudou úspěšně obnoveny všechny správce front klastru a témata klastru, a poté proveďte opětovnou synchronizaci proxy odběrů podle popisu v části [“Resynchronizace proxy odběrů”](#) na stránce 68. Toto uspořádání vyžaduje, aby odesílací kanály klastru byly spouštěny z tohoto správce front do všech ostatních správců front v klastru. Pokud byly všechny odběry proxy správně synchronizovány, restartujte aplikaci publikování/odběru.

Pokud dokončení příkazu **REFRESH CLUSTER** trvá delší dobu, monitorujte ji tak, že se podíváte na CURDEPTH souboru SYSTEM.CLUSTER.COMMAND.QUEUE.

### Související pojmy

[Problémy aplikace zaznamenané při spuštění REFRESH CLUSTER](#)

[Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER](#)

### Související odkazy

[Popis příkazů MQSC: REFRESH CLUSTER](#)

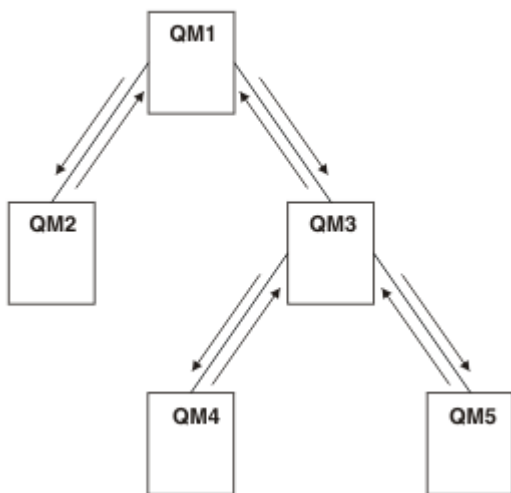
#### *Hierarchie publikování/odběru*

Správci front lze seskupit do hierarchie, kde hierarchie obsahuje jednoho nebo více správců front, kteří jsou přímo připojeni. Správci front jsou připojeni společně s nadřazeným a podřazeným vztahem připojení a času připojení. Jsou-li dva správci front připojeni poprvé, je podřazený správce front připojen k nadřazenému správci front.

Jsou-li nadřazené a podřazené správce front připojeny v hierarchii, mezi nimi není žádný funkční rozdíl, dokud neodpojíte správce front z hierarchie.

**Poznámka:** IBM WebSphere MQ hierarchická připojení vyžadují, aby byl atribut správce front PSMODE nastaven na hodnotu ENABLED.

### Hierarchy



Obrázek 34. Jednoduchá hierarchie publikování/odběru

#### *Připojení správce front k hierarchii zprostředkovatele*

Chcete-li upravit hierarchii zprostředkovatele, můžete připojit lokálního správce front k nadřazenému správci front.

### Než začnete

1. Povolit režim publikování/odběru ve frontě. Viz [Spuštění publikování/odběru ve frontě](#).



2. Tato změna je šířena do nadřazeného správce front pomocí připojení IBM WebSphere MQ . Existují dva způsoby, jak navázat spojení.

- Připojte správce front ke klastru IBM WebSphere MQ . Viz téma [Přidání správce front do klastru](#) .
- Vytvořte připojení kanálu dvoubodového spojení s použitím přenosové fronty nebo aliasu správce front se stejným názvem jako nadřazený správce front. Další informace o způsobu vytvoření dvoubodového připojení kanálu naleznete v tématu [WebSphere MQ techniky distribuovaného systému zpráv](#).

## Informace o této úloze

Pomocí příkazu ALTER QMGR PARENT (*PARENT\_NAME*) runmqsc připojte podřazené prvky k rodičům.

Distribuované publikování/odběr je implementován pomocí klastrů správců front a definic klastrovaných témat. Pro interoperabilitu s produkty IBM WebSphere MQ Version 6.0 a WebSphere Message Broker Version 6.1 a WebSphere Event Broker Version 6.1 a dřívějšími můžete také připojit správce front produktu Version 7.1 nebo novější k hierarchii zprostředkovatele, pokud je povolen režim publikování/odběru ve frontě.

## Postup

```
ALTER QMGR PARENT (PARENT)
```

## Příklad

První příklad ukazuje, jak připojit QM2 jako podřazený prvek QM1a poté se dotazovat QM2 na jeho připojení:

```
C:>runmqsc QM2
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM2
alter qmgr parent(QM1)
  1 : alter qmgr parent(QM1)
AMQ8005: WebSphere MQ queue manager changed.
display pubsub all
  2 : display pubsub all
AMQ8723: Display pub/sub status details.
QMNAME(QM2) TYPE(LOCAL)
STATUS(ACTIVE)
AMQ8723: Display pub/sub status details.
QMNAME(QM1) TYPE(PARENT)
STATUS(ACTIVE)
```

Následující příklad zobrazuje výsledek dotazování QM1 na jeho připojení:

```
C:\Documents and Settings\Admin>runmqsc QM1
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM1.
display pubsub all
  2 : display pubsub all
AMQ8723: Display pub/sub status details.
QMNAME(QM1) TYPE(LOCAL)
STATUS(ACTIVE)
AMQ8723: Display pub/sub status details.
QMNAME(QM2) TYPE(CHILD)
STATUS(ACTIVE)
```

## Jak pokračovat dále

Můžete definovat témata v jednom zprostředkovateli nebo správci front, která jsou k dispozici vydavatelům a odběratelům v připojených správcích front. Další informace naleznete v tématu [Definování administrativního tématu](#) .

### Související pojmy

[Proudy a témata](#)

[Úvod do systému zpráv publikování/odběru produktu WebSphere MQ](#)



## Související odkazy

[ZOBRAZIT PUBSUB](#)

*Odpojení správce front od hierarchie zprostředkovatele*

Odpojte podřízeného správce front od nadřízeného správce front v hierarchii zprostředkovatele.

## Informace o této úloze

Pomocí příkazu **ALTER QMGR** odpojte správce front od hierarchie zprostředkovatele. Správce front můžete kdykoli odpojit v libovolném pořadí.

Příslušný požadavek na aktualizaci nadřízeného prvku je odeslán, když je spuštěno připojení mezi správci front.

## Postup

```
ALTER QMGR PARENT('')
```

## Příklad

```
C:\Documents and Settings\Admin>runmqsc QM2
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM2.
 1 : alter qmgr parent('')
AMQ8005: WebSphere MQ queue manager changed.
 2 : display pubsub type(child)
AMQ8147: WebSphere MQ object not found.
display pubsub type(parent)
 3 : display pubsub type(parent)
AMQ8147: WebSphere MQ object not found.
```

## Jak pokračovat dále

Můžete odstranit všechny proudy, fronty a ručně definované kanály, které již nejsou potřeba.

*Příklad hierarchie publikování/odběru: Scénář 1*

Nastavení topologie hierarchie publikování/odběru pomocí kanálů typu point-to-point s aliasem názvu správce front.

## Informace o této úloze

Tyto scénáře nastavují hierarchii publikování/odběru různými způsoby k vytvoření připojení mezi správci front. Všechny tyto scénáře používají nadřízený správce front s názvem QM1a dva podřízené správce front s názvem QM2a QM3.

Scénář 1 je rozdělen do menších částí, aby bylo možné usnadnit jeho sledování.

*Scénář 1, část 1: Vytvoření správců front*

## Postup

1. Vytvořte a spusťte tři správce front s názvem QM1, QM2a QM3 pomocí následujících příkazů:

```
crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM1
strmqm QM1

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM2
strmqm QM2

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM3
strmqm QM3
```

2. Povolte režim publikování/odběru správce front pomocí následujícího příkazu ve všech třech správcích front:

```
ALTER QMGR PSMODE(ENABLED)
```

## Scenario 1 part 2: Point-to-point channel connections

### Informace o této úloze

Pomocí aliasu správce front se stejným názvem jako nadřizený správce front vytvořte připojení k dvoubodovým kanálům mezi správci front s použitím aliasu správce front.

### Postup

1. Definujte přenosovou frontu a alias správce front v QM2 na QM1. Definujte odesílací kanál pro QM1 a přijímací kanál pro odesílací kanál vytvořený na QM1 pro QM2:

```
DEFINE QLOCAL(QM1.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM1) RNAME('') RQMNAME(QM1) XMITQ(QM1.XMITQ)

DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(RCVR) TRPTYPE(TCP)
```

2. Definujte přenosovou frontu a alias správce front v QM3 na QM1. Definujte odesílací kanál pro QM1 a přijímací kanál pro odesílací kanál vytvořený na QM1 pro QM3:

```
DEFINE QLOCAL(QM1.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM1) RNAME('') RQMNAME(QM1) XMITQ(QM1.XMITQ)

DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(RCVR) TRPTYPE(TCP)
```

3. Definujte přenosovou frontu a alias správce front v systému QM1 na QM2 a QM3. Definujte odesílací kanál pro QM2 a QM3a přijímacího kanálu pro odesílací kanály vytvořené v systémech QM2 a QM3 pro QM1:

```
DEFINE QLOCAL(QM2.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM2) RNAME('') RQMNAME(QM2) XMITQ(QM2.XMITQ)

DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(SDR) CONNAME('localhost(7777)') XMITQ(QM2.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)

DEFINE QLOCAL(QM3.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM3) RNAME('') RQMNAME(QM3) XMITQ(QM3.XMITQ)

DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(SDR) CONNAME('localhost(8888)') XMITQ(QM3.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)
```

4. Spusťte příslušné moduly listener na správci front:

```
runmqclsr -m QM1 -t TCP -p 9999 &
runmqclsr -m QM2 -t TCP -p 7777 &
runmqclsr -m QM3 -t TCP -p 8888 &
```

5. Spusťte následující kanály:

- a. V systému QM1:

```
START CHANNEL('QM1.TO.QM2')

START CHANNEL('QM1.TO.QM3')
```

b. V systému QM2:

```
START CHANNEL('QM2.TO.QM1')
```

c. V systému QM3:

```
START CHANNEL('QM3.TO.QM1')
```

6. Zkontrolujte, zda byly spuštěny všechny kanály:

```
DISPLAY CHSTATUS('QM1.TO.QM2')  
DISPLAY CHSTATUS('QM1.TO.QM3')  
DISPLAY CHSTATUS('QM2.TO.QM1')  
DISPLAY CHSTATUS('QM3.TO.QM1')
```

*Scénář 1 část 3: Spojit správce front a definovat téma*

## Informace o této úloze

Připojte podřízené správce front QM2 a QM3 k nadřízenému správci front QM1.

## Postup

1. V systémech QM2 a QM3 nastavte nadřízeného správce front na hodnotu QM1:

```
ALTER QMGR PARENT (QM1)
```

2. Spuštěním následujícího příkazu na všech správcích front zkontrolujte, zda jsou k nadřízenému správci front připojeni podřízený správce front:

```
DISPLAY PUBSUB TYPE(ALL)
```

3. Definujte objekt tématu:

```
define topic(FOOTBALL) TOPICSTR('Sport/Soccer')
```

*Scénář 1, část 4: Publikování a odběr tématu*

## Informace o této úloze

K publikování a odběru tématu použijte aplikace amqsub.exe a amqssub.exe.

## Postup

1. Spusťte tento příkaz v prvním příkazovém okně:

```
amqsub Sport/Soccer QM2
```

2. Spusťte tento příkaz v druhém příkazovém okně:

```
amqssub Sport/Soccer QM1
```

3. Spusťte tento příkaz ve třetím příkazovém okně:

```
amqssub Sport/Soccer QM3
```

## Výsledky

Aplikace amqssub.exe ve druhém a třetím příkazovém okně přijímají zprávy publikované v prvním příkazovém okně.

## Související úlohy

“Příklad hierarchie publikování/odběru: Scénář 2” na stránce 84

Nastavení topologie hierarchie publikování/odběru pomocí kanálů typu point-to-point s názvem přenosové fronty stejně jako vzdáleného správce front.

“Příklad hierarchie publikování/odběru: Scénář 3” na stránce 86

Přidejte správce front do topologie hierarchie pomocí kanálu klastru.

*Příklad hierarchie publikování/odběru: Scénář 2*

Nastavení topologie hierarchie publikování/odběru pomocí kanálů typu point-to-point s názvem přenosové fronty stejně jako vzdáleného správce front.

## Informace o této úloze

Tyto scénáře nastavují hierarchii publikování/odběru různými způsoby k vytvoření připojení mezi správcem front. Všechny tyto scénáře používají nadřazený správce front s názvem QM1a dva podřazené správce front s názvem QM2a QM3.

Scénář 2 je rozdělen do menších částí, aby bylo možné usnadnit jeho sledování. Tento scénář znovu použije část 1, scénář 1, část 3 a scénář 1, část 4, z [“Příklad hierarchie publikování/odběru: Scénář 1”](#) na stránce 81.

*Scénář 2, část 1: Vytvoření správce front a nastavení PSMODE*

## Postup

1. Vytvořte a spusťte tři správce front s názvem QM1, QM2a QM3 pomocí následujících příkazů:

```
crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM1
strmqm QM1

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM2
strmqm QM2

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM3
strmqm QM3
```

2. Povolte režim publikování/odběru správce front pomocí následujícího příkazu ve všech třech správcích front:

```
ALTER QMGR PSMODE(ENABLED)
```

*Scénář 2, část 2: Připojení kanálů Point-to-point*

## Informace o této úloze

Vytvořte dvoubodová připojení kanálu mezi správcem front pomocí přenosové fronty se stejným názvem, jako má nadřazený správce front.

## Postup

1. Definujte přenosovou frontu v QM2 na QM1. Definujte odesílací kanál pro QM1 a přijímací kanál pro kanál odesílatele pro QM2 vytvořený na serveru QM1:

```
DEFINE QLOCAL(QM1) USAGE(XMITQ)
DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1) TRPTYPE(TCP)
DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(RCVR) TRPTYPE(TCP)
```

2. Definujte přenosovou frontu v QM3 na QM1. Definujte odesílací kanál pro QM1 a přijímací kanál pro odesílací kanál vytvořený na QM1 pro QM3:

```
DEFINE QLOCAL(QM1) USAGE(XMITQ)
DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1) TRPTYPE(TCP)
DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(RCVR) TRPTYPE(TCP)
```

3. Definujte přenosové fronty na QM1 až QM2 a QM3. Definujte odesílací kanály pro QM2 a QM3a přijímací kanál pro odesílací kanály vytvořené v systémech QM2 a QM3 pro QM1:

```
DEFINE QLOCAL(QM2) USAGE(XMITQ)
DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(SDR) CONNAME('localhost(7777)') XMITQ(QM2) TRPTYPE(TCP)
DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)
DEFINE QLOCAL(QM3) USAGE(XMITQ)
DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(SDR) CONNAME('localhost(8888)') XMITQ(QM3) TRPTYPE(TCP)
DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)
```

4. Spusťte příslušné moduly listener na správci front:

```
runmqclsr -m QM1 -t TCP -p 9999 &
runmqclsr -m QM2 -t TCP -p 7777 &
runmqclsr -m QM3 -t TCP -p 8888 &
```

5. Spusťte následující kanály:

- a. V systému QM1:

```
START CHANNEL('QM1.TO.QM2')
START CHANNEL('QM1.TO.QM3')
```

- b. V systému QM2:

```
START CHANNEL('QM2.TO.QM1')
```

- c. V systému QM3:

```
START CHANNEL('QM3.TO.QM1')
```

6. Zkontrolujte, zda byly spuštěny všechny kanály:

```
DISPLAY CHSTATUS('QM1.TO.QM2')
DISPLAY CHSTATUS('QM1.TO.QM3')
DISPLAY CHSTATUS('QM2.TO.QM1')
DISPLAY CHSTATUS('QM3.TO.QM1')
```

*Scénář 2, část 3: Spojit správce front a definovat téma*

## Informace o této úloze

Připojte podřízené správce front QM2 a QM3 k nadřízenému správci front QM1.

## Postup

1. V systémech QM2 a QM3 nastavte nadřízeného správce front na hodnotu QM1:

```
ALTER QMGR PARENT (QM1)
```

2. Spuštěním následujícího příkazu na všech správcích front zkontrolujte, zda jsou k nadřízenému správci front připojeni podřízený správce front:

```
DISPLAY PUBSUB TYPE(ALL)
```

### 3. Definujte objekt tématu:

```
define topic(FOOTBALL) TOPICSTR('Sport/Soccer')
```

Scénář 2, část 4: Publikování a odběr tématu

## Informace o této úloze

K publikování a odběru tématu použijte aplikace `amqspub.exe` a `amqssub.exe`.

## Postup

1. Spusťte tento příkaz v prvním příkazovém okně:

```
amqspub Sport/Soccer QM2
```

2. Spusťte tento příkaz v druhém příkazovém okně:

```
amqssub Sport/Soccer QM1
```

3. Spusťte tento příkaz ve třetím příkazovém okně:

```
amqssub Sport/Soccer QM3
```

## Výsledky

Aplikace `amqssub.exe` ve druhém a třetím příkazovém okně přijímají zprávy publikované v prvním příkazovém okně.

### Související úlohy

[“Příklad hierarchie publikování/odběru: Scénář 1” na stránce 81](#)

Nastavení topologie hierarchie publikování/odběru pomocí kanálů typu point-to-point s aliasem názvu správce front.

[“Příklad hierarchie publikování/odběru: Scénář 3” na stránce 86](#)

Přidejte správce front do topologie hierarchie pomocí kanálu klastru.

*Příklad hierarchie publikování/odběru: Scénář 3*

Přidejte správce front do topologie hierarchie pomocí kanálu klastru.

## Informace o této úloze

Tyto scénáře nastavují hierarchii publikování/odběru různými způsoby k vytvoření připojení mezi správcí front. Všechny tyto scénáře používají nadřazený správce front s názvem QM1a dva podřízené správce front s názvem QM2a QM3.

Scénář 3 je rozdělen na menší části, aby se usnadnil postup. Tento scénář znovu použije část 1, scénář 1, část 3 a scénář 1, část 4, z [“Příklad hierarchie publikování/odběru: Scénář 1” na stránce 81](#).

Tento scénář vytvoří klastr s názvem DEMO, kde QM1 a QM2 jsou úplná úložiště, a QM3 je dílčí úložiště. Správce front QM1 je nadřazený správce front QM2 a QM3.

Scénář 2, část 1: Vytvoření správce front a nastavení PSMODE

## Postup

1. Vytvořte a spusťte tři správce front s názvem QM1, QM2a QM3 pomocí následujících příkazů:

```
crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM1
strmqm QM1

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM2
strmqm QM2
```

```
critmqm -u SYSTEM.DEAD.LETTER.QUEUE QM3
stimqm QM3
```

2. Povolte režim publikování/odběru správce front pomocí následujícího příkazu ve všech třech správci front:

```
ALTER QMGR PSMODE(ENABLED)
```

*Scénář 2, část 2: Připojení kanálu Point-to-point*

## Informace o této úloze

Ustanovte spojení mezi správci front mezi správci front a klastru.

## Postup

1. V systémech QM1 a QM2 nastavte parametr **REPOS** na název klastru DEMO:

```
ALTER QMGR REPOS(DEMO)
```

2. Spusťte příslušné moduly listener na správci front:

```
runmqclsr -m QM1 -t TCP -p 9999 &
runmqclsr -m QM2 -t TCP -p 7777 &
runmqclsr -m QM3 -t TCP -p 8888 &
```

3. Definujte přijímací kanál klastru na každém správci front:

- a. V systému QM1:

```
DEFINE CHANNEL(TO.QM1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('localhost(9999)')
CLUSTER(DEMO)
```

- b. V systému QM2:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('localhost(7777)')
CLUSTER(DEMO)
```

- c. V systému QM3:

```
DEFINE CHANNEL(TO.QM3) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('localhost(8888)')
CLUSTER(DEMO)
```

4. Definujte odesílací kanál klastru do úplného úložiště v každém správci front v klastru:

- a. V systému QM1:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('localhost(7777)')
CLUSTER(DEMO)
```

- b. V systému QM2:

```
DEFINE CHANNEL(TO.QM1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('localhost(9999)')
CLUSTER(DEMO)
```

- c. Produkt QM3 může mít odesílací kanál klastru buď s úplným úložištěm na serveru QM1, nebo QM2. Tento příklad definuje kanál na QM1:

```
DEFINE CHANNEL(TO.QM1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('localhost(9999)')
CLUSTER(DEMO)
```

Scénář 2, část 3: Spojit správce front a definovat téma

## Informace o této úloze

Připojte podřízené správce front QM2 a QM3 k nadřízenému správci front QM1.

## Postup

1. V systémech QM2 a QM3 nastavte nadřízeného správce front na hodnotu QM1:

```
ALTER QMGR PARENT (QM1)
```

2. Spuštěním následujícího příkazu na všech správcích front zkontrolujte, zda jsou k nadřízenému správci front připojeni podřízený správce front:

```
DISPLAY PUBSUB TYPE(ALL)
```

3. Definujte objekt tématu:

```
define topic(FOOTBALL) TOPICSTR('Sport/Soccer')
```

Scénář 2, část 4: Publikování a odběr tématu

## Informace o této úloze

K publikování a odběru tématu použijte aplikace amqsub . exe a amqssub . exe .

## Postup

1. Spusťte tento příkaz v prvním příkazovém okně:

```
amqsub Sport/Soccer QM2
```

2. Spusťte tento příkaz v druhém příkazovém okně:

```
amqssub Sport/Soccer QM1
```

3. Spusťte tento příkaz ve třetím příkazovém okně:

```
amqssub Sport/Soccer QM3
```

## Výsledky

Aplikace amqssub . exe ve druhém a třetím příkazovém okně přijímají zprávy publikované v prvním příkazovém okně.

### Související úlohy

“Příklad hierarchie publikování/odběru: Scénář 1” na stránce 81

Nastavení topologie hierarchie publikování/odběru pomocí kanálů typu point-to-point s aliasem názvu správce front.

“Příklad hierarchie publikování/odběru: Scénář 2” na stránce 84

Nastavení topologie hierarchie publikování/odběru pomocí kanálů typu point-to-point s názvem přenosové fronty stejně jako vzdáleného správce front.

### Řízení toku publikování a odběrů

Správci front, kteří jsou připojeni k distribuované topologii publikování/odběru, sdílejí společný federovaný prostor tématu. Tok publikování a odběrů v rámci topologie můžete řídit tím, že zvolíte, zda jsou jednotlivé publikování a odběry buď lokální, nebo globální.

Lokální publikování a odběry nejsou šířeny mimo správce front, k němuž je vydavatel nebo odběratel připojen.



Rozsah prostorů témat vytvořených připojováním správců front v klastrech nebo hierarchiích můžete řídit rozsah vytvořených prostorů témat. V klastru publikování/odběru, objekt tématu musí být 'klastrovaný' nebo všechny prvky zůstávají lokální a publikování nebo odběr nemají žádný vliv.

Odběr, pokud se shoduje s řetězcí tématu v různých publikacích, může být rozlišen pro různé objekty témat. Ty se nazývají překrývající se témata. Objekt tématu, který je přidružen ke zveřejnění pro konkrétní shodu, poskytuje atributy témat a určuje například, zda má odběratel obdržet publikování.

#### *Obor publikování*

Oblast působnosti publikování řídí, zda správci front přesměroval publikování na vzdálené správce front. K administraci oboru publikování použijte atribut tématu **PUBSCOPE**.

Pokud není publikace předána ke vzdáleným správcům front, obdrží publikování pouze lokální odběratelé.

Atribut tématu **PUBSCOPE** se používá k určení rozsahu publikací vytvořených u specifického tématu. Atribut můžete nastavit na jednu z následujících hodnot:

#### **QMGR**

Publikování je doručeno pouze lokálním odběratelům. Tyto příručky se nazývají *lokální publikace*. Lokální publikace nejsou předávány vzdáleným správcům front, a proto nejsou odběratelé připojeni ke vzdáleným správcům front připojeni.

#### **ALL**

Publikování je doručeno lokálním odběratelům a odběratelům připojeným ke vzdáleným správcům front. Tyto příručky se nazývají *globální publikace*.

#### **AsParent**

Použijte nastavení **PUBSCOPE** nadřazené položky.

Vydavatelé mohou také určit, zda je publikování lokální nebo globální pomocí volby vložení zprávy produktu MQPMO\_SCOPE\_QMGR. Je-li tato volba použita, přepíše jakékoli chování nastavené pomocí atributu tématu **PUBSCOPE**.

#### *Obor odběru*

Rozsah odběru řídí, zda odběr v jednom správci front přijímá publikování publikovaná v jiném správci front v klastru nebo v rámci hierarchie publikování/odběru nebo pouze publikování z lokálních vydavatelů.

Omezení rozsahu odběru na správce front zastaví předávání odběrů serverů proxy jiným správcům front v topologii publikování/odběru. Tím se sníží provoz přenosu zpráv mezi správci front v rámci správce front nebo odběru.

Atribut tématu **SUBSCOPE** se používá k určení rozsahu odběrů, které jsou provedeny na specifickém tématu. Atribut můžete nastavit na jednu z následujících hodnot:

#### **QMGR**

Odběr přijímá pouze lokální publikování a proxy odběry se nešíří do vzdálených správců front.

#### **ALL**

Proxy odběr je šířen na vzdálené správce front a odběratel přijme lokální a vzdálené publikace.

#### **AsParent**

Použijte nastavení **SUBSCOPE** nadřazené položky.

Jednotliví odběratelé mohou potlačit nastavení **SUBSCOPE** hodnoty ALL uvedením volby odběru MQSO\_SCOPE\_QMGR při vytváření odběru. Odběr může přepsat nastavení **SUBSCOPE** tématu ALL.

**Poznámka:** Jednotliví odběratelé mohou omezit pouze **SUBSCOPE** tématu. Má-li individuální odběr nastaven parametr **SUBSCOPE** na hodnotu ALL, bude odběr respektovat nastavení odpovídajících témat **SUBSCOPE**.

#### *Kombinování oborů publikování a odběrů*

V produktu WebSphere MQ verze 7 a obor publikování a odběru pracují nezávisle na určení toku publikací mezi správci front.

Publikování mohou přejít do všech správců front, kteří jsou připojeni k topologii publikování/odběru nebo pouze lokálnímu správci front. Podobně pro proxy odběry. Informace o tom, které publikace odpovídají odběru, se řídí kombinací těchto dvou toků.

Publikování a odběry mohou mít rozsah hodnot QMGR nebo ALL. Pokud je vydavatel a odběratel připojen ke stejnému správci front, neovlivňují nastavení rozsahu publikování, která odběratel obdrží od tohoto vydavatele.

Pokud je vydavatel a odběratel připojeni k různým správcům front, obě nastavení musí být VŠE , aby bylo možné přijímat vzdálená publikování.

Předpokládejme, že vydavatelé jsou připojeni k různým správcům front. Pokud chcete, aby odběratel přijímal publikování od libovolného vydavatele, nastavte rozsah odběru na hodnotu VŠE. Poté můžete rozhodnout pro každého vydavatele, zda má být omezen rozsah jeho publikací na odběratele lokální pro vydavatele.

Předpokládejme, že odběratelé jsou připojeni k různým správcům front. Pokud chcete, aby byly publikace od vydavatele odeslány všem odběratelům, nastavte rozsah publikování na hodnotu VŠE. Chcete-li odběratele přijímat publikování pouze od vydavatele připojeného ke stejnému správci front, nastavte rozsah odběru na QMGR.

Ve verzi 6 a dřívější, publikování a odběru se neřídí pouze publikování, která tekla. Kromě toho se rozsah publikování musel shodovat s rozsahem odběru.

### **Příklad: služba fotbalových výsledků**

Předpokládejme, že jste členský tým ve fotbalové lize. Každý tým má k dispozici správce front připojený ke všem ostatním týmům v klastru publikování/odběru.

Týmy publikují výsledky všech her hraných na jejich domovské zemi pomocí tohoto tématu, `Football/result/Home team name/Away team name`. Řetězce psané kurzívou jsou variabilní názvy témat a publikování je výsledkem shody.

Každý klub také znovu publikuje výsledky pouze pro klub s použitím řetězce tématu `Football/myteam/Home team name/Away team name`.

Obě témata jsou publikována v celém klastru.

Následující odběry byly vytvořeny v lize tak, že fanoušci libovolného týmu se mohou přihlásit k odběru výsledků ve třech zajímavých ohledech.

Všimněte si, že můžete nastavit témata klastru pomocí produktu SUBSCOPE (QMGR). Definice tématu se šíří do každého člena klastru, ale rozsah odběru je pouze lokální správce front. Odběratelé v každém správci front proto obdrží od stejného odběru různé publikace.

### **Přijmout všechny výsledky**

```
DEFINE TOPIC(A) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(ALL)
```

### **Přijmout všechny domovské výsledky**

```
DEFINE TOPIC(B) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR , jsou porovnávány pouze výsledky publikované v domovském umístění.

### **Přijmout všechny výsledky mých týmů**

```
DEFINE TOPIC(C) TOPICSTR('Football/myteam/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR , budou porovnávány pouze lokální výsledky týmu, které se znovu publikují lokálně.

### Prostory tématu

Prostor tématu je sada témat, k jejichž odběru se můžete přihlásit. Odběratel připojený ke správci front v distribuované topologii publikování/odběru má prostor tématu, který potenciálně obsahuje témata definovaná v připojených správcích front.

Témata jsou na počátku vytvořena administrativně při definování objektu tématu nebo trvalého odběru, nebo dynamicky, když aplikace dynamicky vytvoří publikování nebo odběr.

Témata jsou šířena do dalších správců front pomocí proxy odběrů a vytvářením objektů témat administrativního klastru. Proxy odběry mají za následek postoupení publikací od správce front, ke kterému je vydavatel připojen, ke správcům front odběratelů. Proxy odběry jsou mechanismem, podle kterého se témata definovaná v různých správcích front kombinují do společného prostoru tématu.

Odběry proxy se šíří mezi všemi správci front, kteří jsou připojeni k relacím nadřízený-podřízený v hierarchii správce front. Výsledkem je, že se můžete přihlásit k odběru jednoho správce front s použitím tématu definovaného v libovolném jiném správci front v hierarchii. Dokud existuje propojená cesta mezi správci front, nezáleží na tom, jakým způsobem jsou správci front připojeni.

Odběry proxy se také šíří pro témata *klastru* mezi všemi členy klastru. Téma klastru je téma, které je připojeno k objektu tématu, který má atribut **CLUSTER**, nebo který dědí atribut z jeho nadřazené položky. Témata, která nejsou témata klastru, jsou známa jako lokální témata a nereplikují se do klastru. Do klastru z odběrů na lokální témata nejsou šířeny žádné odběry proxy.

Chcete-li shrnout, proxy odběry jsou vytvářeny pro odběratele za dvou okolností.

1. Správce front je členem hierarchie a proxy odběr je předáván nadřízenému a podřízenému objektu správce front.
2. Správce front je členem klastru a řetězec tématu odběru se přeloží na téma, které je přidruženo k objektu tématu klastru. Odběry proxy jsou přesměrovány na všechny členy klastru. Další informace o komplikacím najdete v příručce [“Překrývání témat”](#) na stránce 99.

Je-li správce front členem klastru a hierarchie, proxy odběry jsou šířeny oběma mechanismy, aniž by doručíte duplicitní publikace odběrateli.

Efekt vytvoření objektu tématu klastru je dvojitý. Odběry proxy pro téma jsou odeslány ostatním členům klastru, když se odběr vyřeší na téma klastru. Odešle také kopii objektu tématu do ostatních členů klastru. Cílem objektů témat klastru je zjednodušit administraci témat. Typicky jsou objekty tématu klastru definovány v jednom správci front v klastru, označovaný jako hostitel tématu klastru.

Témata se třemi topologiemi publikování/odběru jsou popsány v následujícím seznamu:

- [“Případ 1. Klastry publikování/odběru”](#) na stránce 91.
- [“Případ 2. Hierarchie publikování/odběru ve verzi 7”](#) na stránce 93.
- [“Případ 3. Hierarchie publikování/odběru a proudy ve verzi 6”](#) na stránce 93.

V samostatných tématech popisují následující úlohy, jak kombinovat prostory témat.

- [“Vytvoření jediného prostoru tématu v klastru publikování/odběru”](#) na stránce 93.
- [“Přidat správce front verze 7 k existujícím prostorům témat verze 6”](#) na stránce 94.
- [“Kombinování prostorů tématu s více klastry”](#) na stránce 95.
- [“Kombinování a izolování prostorů témat ve více klastrech”](#) na stránce 97
- [“Publikování a přihlášení k odběru prostorů témat ve více klastrech”](#) na stránce 98

### Případ 1. Klastry publikování/odběru

V tomto příkladu předpokládáme, že správce front *není* připojen k hierarchii publikování/odběru.

Je-li správce front členem klastru publikování/odběru, je jeho prostor tématu vytvořen z lokálních témat a témat klastru. Lokální témata jsou přidružena k objektům tématu bez atributu **CLUSTER**. Pokud má správce front definice objektů lokálního tématu, jeho prostor tématu se liší od jiného správce front v klastru, který má také vlastní lokálně definované objekty témat.

V klastru publikování/odběru se nemůžete přihlásit k odběru tématu definovaného v jiném správci front, pokud se nezahlásíte, že se přihlásíte k odběru objektu tématu klastru.

Konfliktní definice tématu klastru, které jsou definovány jinde v klastru, jsou vyřešeny ve prospěch nejnovější definice. V libovolném časovém okamžiku, pokud bylo téma klastru definováno vícekrát, může být definice tématu klastru v různých správcích front odlišná.

Lokální definice objektu tématu, ať už definice je pro téma klastru nebo lokální téma, má přednost před stejným objektem tématu definovaným jinde v klastru. Používá se lokálně definované téma, a to i v případě, že je objekt definovaný na jiném místě novější.

Nastavte některou z voleb **PUBSCOPE** a **SUBSCOPE** na hodnotu QMGR, aby se zabránilo publikování nebo odběru v tématu klastru, které proudí do různých správců front v klastru.

Předpokládejme, že jste definovali objekt tématu klastru Alabama s řetězcem tématu USA/Alabama na hostiteli témat klastru. Výsledek je následující:

1. Prostor tématu v rámci hostitele tématu klastru nyní obsahuje objekt tématu klastru Alabama a téma USA/Alabama.
2. Objekt tématu klastru Alabama je replikován na všechny správce front v klastru, kde je zkombinován s prostorem tématu v každém správci front. To, co se stane u každého správce front v klastru, závisí na tom, zda objekt tématu Alabama existuje ve správci front.
  - Je-li Alabama novým objektem tématu, přidá správce front objekt tématu klastru Alabama a téma USA/Alabama do prostoru tématu.
  - Je-li Alabama lokální definicí, je přidán objekt tématu klastru Alabama. Pokud není lokální definice odstraněna, objekt tématu klastru vzdáleně definovaný se ignoruje. Správce front zachovává obě definice.
  - Je-li Alabama starší objekt tématu klastru definovaný jinde, je nahrazen novějším objektem tématu klastru.
3. Aplikace nebo administrátor, kdekoli v klastru, může vytvořit odběr produktu USA/Alabama odkazem na objekt tématu Alabama.
4. Aplikace, kdekoli v klastru, pomocí řetězce tématu USA/Alabama přímo může vytvořit odběr, který zdědí atributy objektu tématu Alabama. Objekt tématu Alabama je zděděn z odběru vytvořeného ze všech řetězců témat začínajících řetězcem USA/Alabama,

Existuje-li jiná definice objektu tématu Alabama v jednom z ostatních správců front, bude mít přednost před definicí na hostiteli tématu klastru. Lokální objekt může mít atribut klastru, nebo nemusí. Atribut klastru může odkazovat na stejný klaster nebo jiný klaster. Zkuste se vyhnout těmto případům s více definicemi. Vedou k rozdílným v chování.

5. Pokud má objekt tématu Alabama atribut **PUBSCOPE** ALL, odběry, které se interpretují jako Alabama, jsou odeslány všem ostatním správcům front v klastru.

Nastavte atribut Alabama **PUBSCOPE** na hodnotu QMGR, čímž zabráníte tomu, aby publikování proudilo od vydavatelů k odběratelům připojenému k různým správcům front v klastru byl připojen.

Objekt tématu Alabama je replikován do všech správců front v klastru, takže atributy **PUBSCOPE** a **SUBSCOPE** se vztahují na všechny správce front v klastru.

Je důležité, aby objekt tématu klastru byl přidružen ke stejnému tématu tématu kdekoli v klastru. Řetězec tématu, ke kterému je přidružen objekt tématu, nelze změnit. Chcete-li přidružit stejný objekt tématu k jinému řetězci tématu, je třeba objekt tématu odstranit a znovu jej vytvořit s použitím nového řetězce tématu. Je-li téma klastrováno, je výsledkem odstranění kopií objektu tématu uloženého na ostatních členech klastru a následné vytvoření kopií nového objektu tématu kdekoli v klastru. Kopie objektu tématu se všechny odkazují na stejný řetězec tématu.

Můžete však vytvořit duplicitní definici objektu tématu v jiném správci front v daném klastru s jiným řetězcem tématu. Při správě hostitelů témat klastru v jednom správci front se vždy pokuste vyhnout duplikátům. Další informace o tomto důležitém bodu naleznete v příručce [“Více definic témat klastru”](#) na stránce 70. Několik definic stejného objektu tématu s různými řetězci témat může vytvářet různé výsledky v závislosti na tom, jak a kde se na toto téma odkazuje.

## Případ 2. Hierarchie publikování/odběru ve verzi 7

V tomto příkladu předpokládáme, že správce front *není* členem klastru publikování/odběru.

Pokud je správce front členem hierarchie publikování/odběru, ve verzi 7 se jeho prostor tématu skládá ze všech témat definovaných lokálně a na připojených správcích front. Prostor tématu všech správců front v hierarchii je stejný. Do lokálních témat a témat klastru se nerozděluje žádná témata.

Nastavte některou z voleb **PUBSCOPE** a **SUBSCOPE** na hodnotu QMGR, abyste zabránili publikování v tématu toku z vydavatele na odběratele připojeného k různým správcům front v hierarchii.

Předpokládáme, že jste definovali objekt tématu Alabama s řetězcem tématu USA/Alabama ve správci front QMA. Výsledek je následující:

1. Prostor tématu v QMA nyní obsahuje objekt tématu Alabama a řetězec tématu USA/Alabama.
2. Aplikace nebo administrátor může vytvořit odběr v QMA pomocí objektu tématu s názvem Alabama.
3. Aplikace může vytvořit odběr pro libovolné téma, včetně produktu USA/Alabama, do libovolného správce front v hierarchii. Pokud nebyla položka QMA lokálně definována, bude téma USA/Alabama interpretováno jako objekt tématu SYSTEM.BASE.TOPIC.

## Případ 3. Hierarchie publikování/odběru a proudy ve verzi 6

Před verzí 7 se prostor tématu rozdělil do samostatných proudů, které obsahovaly výchozí proud, který byl přítomen ve všech správcích front. Publikování nemohou přecházet mezi různými proudy. Pokud jsou použity pojmenované toky dat, mohou být různé prostory témat v různých správcích front odlišné. Témata jsou rozdělena na témata ve výchozím proudu a témata v různých pojmenovaných proudech.

**Poznámka:** Každý pojmenovaný proud tvoří samostatný prostor tématu. Chcete-li vytvořit připojenou topologii, každý pojmenovaný proud musí existovat v připojených správcích front. Předpokládáme, že proud X je definován na QMA a QMC, ale ne na QMB. Pokud je QMA nadřazeným prvkem QMBa QMB je nadřazený QMC, žádná témata v proudu X nemohou přecházet mezi QMA a QMC.

Nastavení obou voleb **PUBSCOPE** a **SUBSCOPE** buď na hodnotu QMGR, nebo na hodnotu ALL vyžaduje, aby vydavatel a odběratel na téma vyměnili pouze publikace pro lokální spotřebu, nebo aby si vyměnili pouze publikace pro globální spotřebu.

Od verze 7 nejsou proudy k dispozici prostřednictvím rozhraní API pro publikování a odběr. Pokud používáte publikování/odběr ve frontě ve správci front verze 7, proudy jsou mapovány na různé objekty témat, které mohou simulovat účinek proudů. Proud je simulován vytvořením objektu tématu, který je kořenovým tématem pro všechna témata v proudu. Správce front mapuje publikování a odběry mezi proudem a příslušným kořenovým tématem každého stromu.

### *Kombinování prostorů témat*

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Můžete vytvořit různé prostory témat publikování/odběru pomocí stovebních bloků atributů **CLUSTER**, **PUBSCOPE** a **SUBSCOPE**, klastrů typu publikování/odběr a publikování/odběru hierarchií.

Při spuštění z příkladu změny měřítka z jednoho správce front do klastru publikování/odběru, následující scénáře ilustrují různé topologie publikování/odběru.

### *Vytvoření jediného prostoru tématu v klastru publikování/odběru*

Rozšiřte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

## Než začnete

Naimplementovali jste systém typu publikování-odběr u jednoho správce front verze 7.

Vždy vytvářejte prostory tématu s vlastními uživateli root, spíše než spoléháte na dědění atributů produktu SYSTEM.BASE.TOPIC. Pokud škálujete systém publikování/odběru do klastru, můžete

definovat kořenové témata jako témata klastru, na hostiteli témat klastru a poté všechny vaše témata sdílet v rámci celého klastru.

## Informace o této úloze

Nyní chcete rozšířit systém tak, aby podporoval více vydavatelů a odběratelů a aby měl každé téma viditelné v rámci celého klastru.

## Postup

1. Vytvořte klastr, který má být použit se systémem publikování/odběru.  
Máte-li existující tradiční klastr, z důvodu výkonu je lepší nastavit nový klastr pro nový systém odběru publikování. Pro úložiště klastru u obou klastrů můžete použít stejné servery.
2. Vyberte jednoho správce front, pravděpodobně jednoho z úložišť, který bude hostitelem tématu klastru.
3. Ujistěte se, že každé téma, které má být viditelné v rámci klastru publikování/odběru, se interpretuje jako objekt tématu administrace.  
Nastavte atribut **CLUSTER** pro pojmenování klastru publikování/odběru.

## Jak pokračovat dále

Připojte vydavatele a aplikace odběratele do všech správců front v klastru.

Vytvořte objekty administrativního tématu, které mají atribut **CLUSTER**. Témata se také šíří do celého klastru. Programy vydavatele a odběratele používají administrativní témata, aby jejich chování nebylo změněno tím, že je připojeno k různým správcům front v klastru.

Pokud potřebujete produkt `SYSTEM.BASE.TOPIC` v každém správci front vystupovat jako téma klastru, je třeba jej upravit ve všech správcích front.

*Přidat správce front verze 7 k existujícím prostorům témat verze 6*

Rozšířte existující systém publikování/odběru verze 6 tak, aby pracoval se správcem front verze 7 a sdílel stejné prostory témat.

## Než začnete

Máte existující systém publikování/odběru verze 6.

Nainstalovali jste produkt WebSphere MQ verze 7 na nový server a nakonfigurovali jste správce front.

## Informace o této úloze

Chcete rozšířit existující systém publikování/odběru verze 6 tak, aby pracoval se správcem front verze 7.

Rozhodli jste se stabilizovat vývoj systému publikování/odběru verze 6, který používá rozhraní publikování/odběru ve frontě. Zamýšlíte přidat rozšíření do systému pomocí rozhraní MQI verze 7. Nyní nemáte žádné plány na přepsání aplikací publikování/odběru ve frontě.

Máte v úmyslu upgradovat správce front verze 6 na verzi 7 v budoucnu. Prozatím nadále spouštíte existující aplikace publikování/odběru ve frontě ve správcích front verze 7.

## Postup

1. Vytvořte jednu sadu kanálů příjemce odesílatele k připojení správce front verze 7 k jednomu z správců front verze 6 v obou směrech.
2. Vytvořte dvě přenosové fronty s názvy cílových správců front. Alias správce front použijte, pokud z nějakého důvodu nelze použít název cílového správce front jako název přenosové fronty.
3. Konfigurujte přenosové fronty tak, aby spustily odesílací kanály.

4. Pokud systém publikování/odběru verze 6 používá proudy, přidejte proudy do správce front verze 7, jak je popsáno v tématu [Přidání proudu](#).
5. Zkontrolujte, zda je správce front verze 7 **PSMODE** nastaven na hodnotu ENABLE.
6. Změňte její atribut **PARENT** tak, aby odkazoval na jednoho ze správců front verze 6.
7. Zkontrolujte, zda je stav relace nadřizený-podřizený mezi správcí front aktivní v obou směrech.

## Jak pokračovat dále

Po dokončení úlohy sdílí správce front verze 6 i verze 7 stejné prostory témat. Můžete například provést všechny následující úlohy.

- Vyměňujte publikace a odběry mezi správcí front verze 6 a verze 7.
- Spusťte své stávající programy publikování/odběru verze 6 ve správcí front verze 7.
- Zobrazte a upravte prostor tématu buď ve správcí front verze 6 nebo verze 7.
- Zapisovat a spouštět aplikace pro publikování a odběr verze 7 a spouštět je ve správcí front verze 7.
- Vytvářejte nové publikace a odběry s aplikacemi verze 7 a vyměňujete je s aplikacemi verze 6.

### *Kombinování prostorů tématu s více klastry*

Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

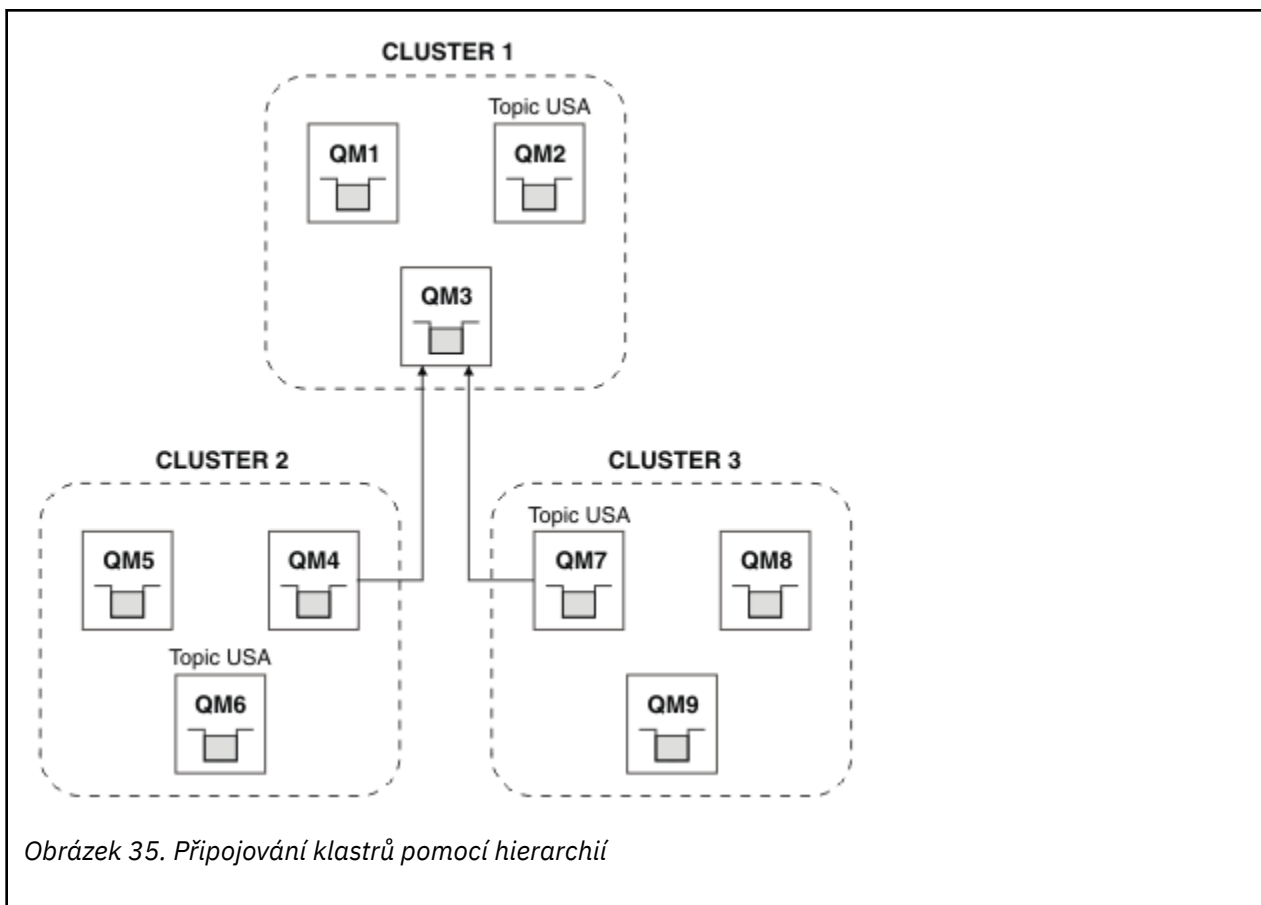
## Než začnete

Máte existující klastry publikování/odběru, a chcete šířit některá témata klastru do všech klastrů.

## Informace o této úloze

Chcete-li šířit publikace z jednoho klastru do jiného, musíte se připojit ke klastrům společně v hierarchii. Další informace naleznete v tématu [Obrázek 35 na stránce 96](#). Hierarchická připojení šíří odběry a publikování mezi propojenými správcí front a klastry šíří témata klastru v rámci jednotlivých klastrů, ale nikoli mezi klastry.

Kombinace těchto dvou mechanismů šíří témata klastru mezi všemi klastry. Je třeba, abyste v každém klastru zopakovali definice tématu klastru.



Obrázek 35. Připojování klastrů pomocí hierarchií

Následující kroky spojují klastry do hierarchie.

## Postup

1. Vytvořte dvě sady přijímacích kanálů odesílatele k připojení produktů QM3 a QM4 a QM3 a QM7v obou směrech. Chcete-li připojit hierarchii, musíte použít tradiční odesílací kanály odesílatele a přenosové fronty, spíše než klastr.
2. Vytvořte tři přenosové fronty s názvy cílových správců front. Alias správce front použijte, pokud z nějakého důvodu nelze použít název cílového správce front jako název přenosové fronty.
3. Konfigurujte přenosové fronty tak, aby spustily odesílací kanály.
4. Zkontrolujte, zda je **PSMODE** z QM3, QM4 a QM7 nastaveno na ENABLE.
5. Pozměňte atribut **PARENT** z QM4 a QM7 na QM3.
6. Zkontrolujte, zda je stav relace nadřízený-podřízený mezi správcí front aktivní v obou směrech.
7. Vytvořte administrativní téma USA s atributem **CLUSTER**(' CLUSTER 1 '), **CLUSTER**(' CLUSTER 2 ') a **CLUSTER**(' CLUSTER 3 ') na každém ze tří hostitelů témat klastru v klastrech 1, 2 a 3. Hostitele tématu klastru nemusí být hierarchicky připojeným správcem front.

## Jak pokračovat dále

Nyní můžete publikovat nebo přihlásit se k odběru tématu klastru USA v produktu [Obrázek 35 na stránce 96](#). Publikování odběrů publikování pro vydavatele a odběratele ve všech třech klastrech.

Předpokládejme, že jste nevytvořili USA jako téma klastru v ostatních klastrech. Je-li USA definováno pouze v systému QM7, jsou publikace a odběry USA vyměňovány mezi QM7, QM8, QM9a QM3. Vydavatelé a odběratelé spuštění v systému QM7, QM8, QM9 dědí atributy administrativního tématu USA. Vydavatelé a odběratelé na QM3 dědí atributy z SYSTEM.BASE.TOPIC na QM3.



*Kombinování a izolování prostorů témat ve více klastrech*

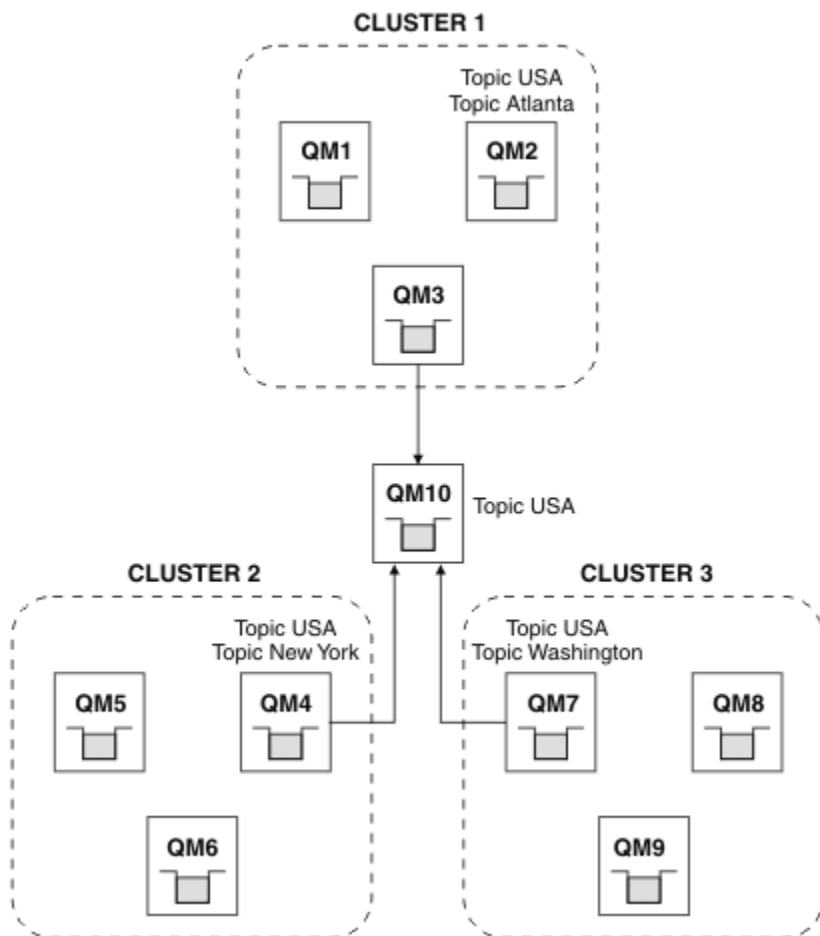
Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

## Než začnete

Proveďte téma “Kombinování prostorů tématu s více klastry” na stránce 95. Může to být dostačující pro vaše potřeby, aniž byste přidali dalšího správce front jako most.

## Informace o této úloze

Potenciální zlepšení topologie zobrazené v produktu [Obrázek 35 na stránce 96](#) v produktu “Kombinování prostorů tématu s více klastry” na stránce 95 spočívá v izolaci témat klastru, která nejsou sdílena mezi všemi klastry. Izolovat klastry vytvořením přemostovacího správce front, který není v žádném z klastrů; viz [Obrázek 36 na stránce 97](#). Pomocí správce front pro přemostění můžete filtrovat, které publikace a odběry mohou přecházet z jednoho klastru do jiného.



Obrázek 36. Propojené klastry

Pomocí mostu určete témata klastru, která nechcete vystavit na základě mostu na ostatních klastrech. V produktu [Obrázek 36 na stránce 97](#) je USA téma klastru sdílené ve všech klastrech a produkty Atlanta, New York a Washington jsou témata klastru, která jsou sdílena pouze v jednom klastru.

Modelujte konfiguraci pomocí následující procedury:

## Postup

1. Upravte všechny objekty témat SYSTEM.BASE.TOPIC tak, aby měly všechny správce front **SUBSCOPE(QMGR)** a **PUBSCOPE(QMGR)**.

Žádná témata (ani témata klastru) se nešíří do jiných správců front, pokud jste explicitně nenastavili **SUBSCOPE(ALL)** a **PUBSCOPE(ALL)** na kořenové téma témat klastru.

2. Definujte témata na třech hostitelích témat klastru, která chcete sdílet v každém klastru s atributy **CLUSTER(clustername)**, **SUBSCOPE(ALL)** a **PUBSCOPE(ALL)**.

Chcete-li některá témata klastru sdílet mezi všemi klastry, definujte stejné téma v každém z klastrů. Jako atribut klastru použijte název klastru každého klastru.

3. V případě témat klastru, která chcete sdílet mezi všemi klastry, definujte témata znovu ve správci front mostu (QM10) s atributy **SUBSCOPE(ALL)** a **PUBSCOPE(ALL)**.

### Příklad

V příkladu v produktu [Obrázek 36 na stránce 97](#) se šíří pouze témata, která dědí od USA mezi všemi třemi klastry.

### Jak pokračovat dále

Odběry pro témata definovaná ve správci front mostu s produktem **SUBSCOPE(ALL)** a **PUBSCOPE(ALL)** jsou šířeny mezi klastry.

Odběry pro témata definovaná v rámci každého klastru s atributy **CLUSTER(clustername)**, **SUBSCOPE(ALL)** a **PUBSCOPE(ALL)** jsou šířeny v rámci každého klastru.

Všechny ostatní odběry jsou lokální pro správce front.

*Publikování a přihlášení k odběru prostorů témat ve více klastrech*

Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

### Než začnete

Vytvořte více tradičních klastrů s některými správci front v průsečících mezi klastry.

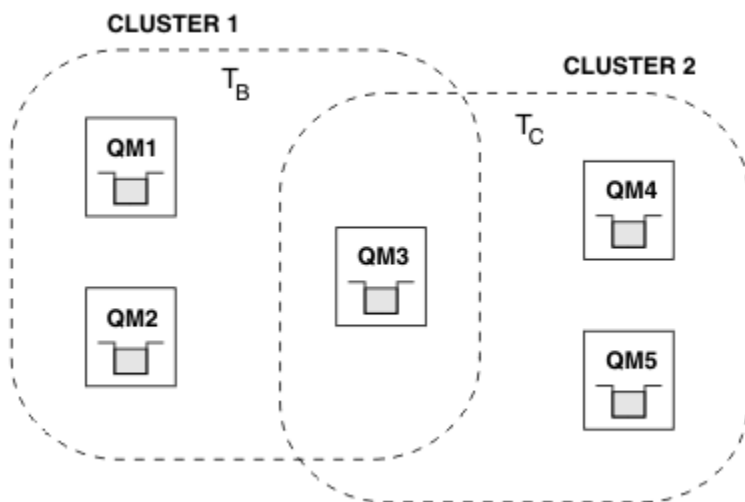
### Informace o této úloze

Možná jste se rozhodli překrývat klastry pro různé různé důvody.

1. Máte omezený počet serverů s vysokou dostupností nebo správců front. Rozhodli jste se implementovat všechna úložiště klastru a hostitele klastru k nim.
2. Máte existující klastry tradičních správců front, které jsou připojeny pomocí správců front brány. Chcete implementovat aplikace publikování/odběru do stejné topologie klastru.
3. Máte několik samostatně obsažených aplikací typu publikování/odběr. Z výkonnostních důvodů je lepší udržovat malé a oddělené klastry publikování/odběru odděleně od tradičních klastrů. Rozhodli jste se implementovat aplikace do různých klastrů. Avšak také chcete monitorovat všechny aplikace publikování/odběru na jednom správci front, protože jste licencovali pouze jednu kopii aplikace monitorování. Tento správce front musí mít přístup k publikacím na témata klastru ve všech klastrech.

Tím, že zajistíte, aby vaše témata byla definována v nepřekrývaných prostorech témat, můžete implementovat témata do překrývajících se klastrů publikování/odběru, viz [Obrázek 37 na stránce 99](#). Pokud se mezery tématu překrývají, pak implementace do překrývajících se klastrů bude mít za následek problémy.

Vzhledem k tomu, že klastry publikování/odběru se překrývají, můžete publikovat a odebírat kterýkoli z prostorů témat používajících správce front v překryvu.



Obrázek 37. Překrývající se klastry, nepřekrývající se prostory tématu

## Postup

Vytvořte prostředek, který zajistí, aby se prostory tématu nepřekrývaly.

Například definujte jedinečné kořenové téma pro každý z prostorů témat. Témata týkající se klastru kořenových témat provedte jako témata.

- a) DEFINE TOPIC(B) TOPICSTR('B') CLUSTER('CLUSTER 1') ...
- b) DEFINE TOPIC(C) TOPICSTR('C') CLUSTER('CLUSTER 2') ...

## Příklad

V produktu [Obrázek 37 na stránce 99](#) vydavatelé a odběratel, který je připojen k produktu QM3, může publikovat nebo odebírat  $T_B$  nebo  $T_C$

## Jak pokračovat dále

Navázat vydavatele a odběratele, kteří používají témata v obou klastrech pro správce front v překryvu.

Připojte vydavatele a odběratele, kteří musí používat pouze témata ve specifickém klastru pro správce front, kteří nejsou v překryvu.

### Překrývání témat

Překrývající se témata se objevují, když může být publikace přidružena k různým objektům tématu, v závislosti na distribuované topologii publikování/odběru, publikování a v řetězcích témat odběru.

Překrývající se mezi tématy musí být zvažována, pokud by bylo možné téma vyřešit na více než jeden objekt tématu.

### Lokální témata v klastru

Téma může být definováno na libovolném správci front v klastru. Je-li téma definováno lokálně, má přednost před tématem klastru, které je definováno jinde, a interpretuje se na stejný řetězec tématu.

### Témata klastru v klastru

Téma může být definováno na libovolném správci front v klastru. Je-li téma klastrováno, replikuje se na ostatní členy klastru. Je-li téma definováno jako téma klastru v jiném správci front v klastru, jedná se o chybu. Do protokolu chyb správce front, který má existující definici klastru, se zapíše chybová zpráva.

Jako pravidlo definujte témata klastru pouze pro jednoho správce front v klastru, "hostitel témat klastru", abyste se ujistili, že existuje pouze jedna definice tématu klastru.

Pokud znovu definujete téma klastru, změna se projeví až po dosažení každého správce front. Poslední definice nakonec přepíše dřívější definice témat klastru, které byly replikovány na neklastrové hostitele témat.

Pokud definujete téma klastru na více správcích front v klastru s různými atributy, nejnovější definice nepřepíše žádné dřívější lokální definice.

### Odběry zástupných znaků pro více řetězců témat

Pokud odběr obsahuje zástupné znaky, mohou potenciálně různá témata v prostoru tématu odpovídat odběru a mohou vést k vyřešení odběru pro různé objekty témat.

Předpokládejme například následující definice témat v klastru SPORTS.

```
DEFINE TOPIC(A) TOPICSTR('Football/result/#') SUBSCOPE(QMGR) CLUSTER(SPORTS)
DEFINE TOPIC(B) TOPICSTR('Football/#') SUBSCOPE(ALL) CLUSTER(SPORTS)
DEFINE TOPIC(C) TOPICSTR('Football/result/Newport/Cardiff') PUBSCOPE(ALL) SUBSCOPE(ALL)
CLUSTER(SPORTS)
DEFINE TOPIC(D) TOPICSTR('Football/matches/Newport/Cardiff') PUBSCOPE(ALL) SUBSCOPE(QMGR)
CLUSTER(SPORTS)
```

Předpokládejme, že v klastru jsou dva správci front QM1 a QM2 . Témata C a D jsou publikována na QM1.

Pokud jsou tyto odběry neseskupené, uvažte o tom, co obdrží odběratel v systému QM2 .

- Odběr tématu A nepřijímá nic.
  - SUBSCOPE (QMGR) a publikování je na druhém správci front.
- Odběr tématu B přijímá obě publikace.
  - SUBSCOPE (ALL) a PUBSCOPE (ALL) v obou případech.
- Odběr tématu C přijímá jednu publikaci.
  - SUBSCOPE (ALL) a PUBSCOPE (ALL) , a shoda s publikací na téma C.
- Odběr tématu D nepřijímá nic.
  - SUBSCOPE (QMGR) a publikování je na druhém správci front.

Pokud jsou tyto odběry seskupeny, zvažte, co přijímá odběratel na QM2 .

- Odběratel obdrží jedno publikování na téma C.
  - Odpovídající odběr u tématu A s produktem SUBSCOPE (QMGR) je potlačen pomocí odpovídajícího odběru u tématu C s produktem SUBSCOPE (ALL) . Vyhrává se specifitější odběr a je obdrženo publikování.
  - Odpovídající odběr u tématu B je odmítnut ve prospěch odběru odpovídajícího odběru u tématu C, protože odběry jsou seskupeny a C je specifitější. Duplicitní publikování je zrušeno.
- Odběratel neobdrží žádné publikování na téma D
  - Odpovídající odběr u tématu B s produktem SUBSCOPE (ALL) je potlačen pomocí odpovídajícího odběru u tématu D s produktem SUBSCOPE (QMGR) . Vyhrává se specifitější odběr a publikování je zrušeno.

### ***Jak detekce smyčky funguje***

V distribuované síti publikování/odběru je důležité, aby publikování a proxy odběry nemohly být zacyklení, protože by to vedlo k zaplavené síti s připojenými odběrateli, kteří obdrží více kopií stejné původní publikace.

Agregační systém odběru proxy popsáný v produktu *“Agregace odběru proxy a agregace publikování”* na stránce 51 nebrání vytvoření smyčky, ačkoli zabrání ve vytváření trvalých cyklů proxy odběrů. Vzhledem k tomu, že šíření publikací je určováno existencí proxy odběrů, mohou tyto publikace vstupovat do nekonečného cyklu. Produkt Websphere MQ V7.0 používá následující techniky k zabránění toho, aby publikace byly trvale zacyklené:

Při přesouvání publikování v rámci topologie publikování/odběru každý správce front přidá jedinečný otisk prstu do záhlaví zprávy. Kdykoli správce front publikování/odběru přijme publikování z jiného správce front

publikování/odběru, budou zkontrolovány otisky prstů obsažené v záhlaví zprávy. Je-li již jeho vlastní otisk prstu přítomen, publikace se zcela rozešle okolo cyklu, takže správce front zprávu vyřadí a přidá záznam do protokolu chyb.

**Poznámka:** V rámci smyčky jsou publikace šířeny v obou směrech ve smyčce a každý správce front v rámci cyklu obdrží obě publikace, než původní správce front vyřadí zacyklené publikace. Výsledkem jsou odebírající aplikace, které přijímají duplicitní kopie publikací, do té doby, než bude smyčka přerušena.

#### *Formát otisku prstu zjišťování smyčky*

Otisky prstů rozpoznání smyčky se vkládají do záhlaví nebo toku RFH2 jako součást protokolu V7.0 . Je třeba, aby programátor RFH2 rozuměl záhlaví a předal informace o otiscích prstů nedotčené. Produkt WebSphere MessageBroker používá záhlaví RFH1 , která nebudou obsahovat informace o otiscích prstů.

```
<ibm>
  <Rfp>uuid1</Rfp>
  <Rfp>uuid2</Rfp>
  <Rfp>uuid3</Rfp>
</ibm>
```

< ibm> je název složky, která obsahuje seznam otisků prstů, které obsahují jedinečný identifikátor uživatele (uuid) každého správce front, který byl navštíven.

Pokaždé, když správce front publikuje zprávu, přidá její uuid do složky < ibm> pomocí značky < Rfp> (směrování otisku prstu). Kdykoli je publikace přijata, produkt WebSphere MQ použije rozhraní API vlastností zprávy k iterování přes značky < Rfp >, aby zjistil, zda je přítomna konkrétní hodnota uuid. Vzhledem k tomu, že komponenta WebSphere Platform Messaging produktu WebSphere MQ se připojuje k produktu Websphere Message Broker prostřednictvím kanálu a odběru RFH2 při použití rozhraní publikování/odběru ve frontě, produkt WebSphere MQ také vytvoří otisk prstu, jakmile obdrží publikování touto trasou.

Cílem je nedodat žádné RFH2 do aplikace, pokud to neočekává žádné, prostě proto, že jsme přidali informace o otiscích prstů.

Kdykoli se RFH2 převede na vlastnosti zprávy, bude také nutné převést složku < ibm>; tím se odstraní informace o otiscích prstů z RFH2 , které jsou předány nebo doručeny aplikacím, které používají rozhraní API prostředí Websphere MQ V7.0 .

Kdykoli je zpráva, která má informace o otiscích prstů, předána odběrateli RFH1 nebo je předána na produkt Websphere Message Broker V6.0, jsou informace o otiscích prstů převedeny na RFH1.

Když produkt Websphere Message Broker V6.0 předá tuto zprávu odběrateli RFH2 , jako je SIB, musí se informace o otisku prstu převést zpět na formát RFH2 .

Aplikace platformy JMS nevidí informace o otiscích prstů, protože rozhraní JMS neextrahuje tyto informace z RFH2, a proto ji ručně nepředá do svých aplikací.

Vlastnosti zprávy Rfp se vytvářejí pomocí produktu propDesc.CopyOptions = MQCOPY\_FORWARD and MQCOPY\_PUBLISH. To má vliv na aplikace, které přijímají a pak znovu publikují stejnou zprávu. Znamená to, že taková aplikace může pokračovat v řetězci směrování otisků prstů pomocí produktu PutMsgOpts.Action = MQACTP\_FORWARD, ale musí být zakódována odpovídajícím způsobem, aby bylo možné odebrat vlastní otisk prstu z řetězu. Aplikace standardně používá produkt PutMsgOpts.Action = MQACTP\_NEW a spouští nový řetězec.

#### **Zachovaná publikování v topologii distribuovaného publikování/odběru**

Při použití zachovaného publikování v distribuované topologii publikování/odběru je nejlepším způsobem publikovat pouze zachované publikace na stejném tématu z jediného správce front v topologii.

Jinak je možné, že různé zachované publikace mohou být aktivní v různých správcích front pro stejné téma, což vede k neočekávanému chování. Jelikož se distribuuje více odběrů proxy, může být přijato více zachovaných publikování.

## Zabezpečení publikování/odběru mezi správci front

Interní zprávy publikování/odběru, jako jsou například proxy odběry a publikace, jsou vloženy do systémových front publikování/odběru s použitím běžných pravidel zabezpečení kanálu. Informace a diagramy v tomto tématu zdůrazňují různé procesy a ID uživatelů, které se podílejí na doručování těchto zpráv.

### Lokální řízení přístupu

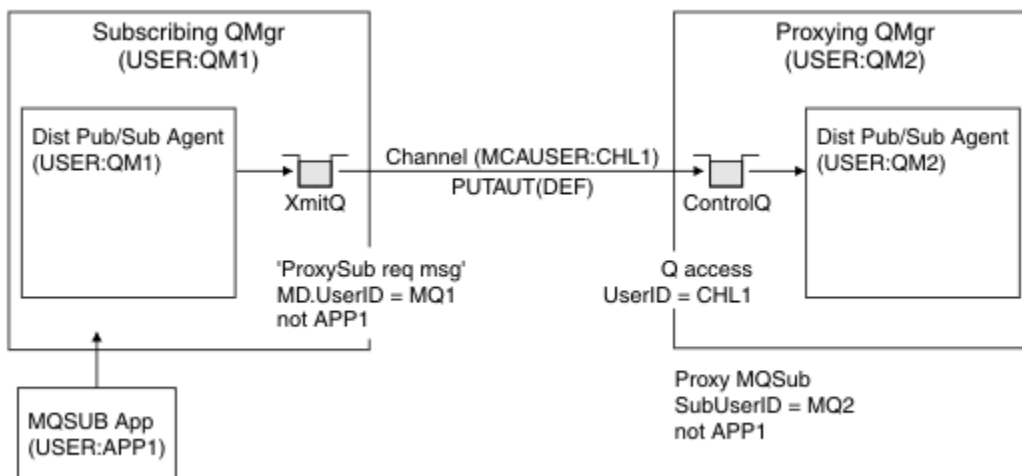
Přístup k tématům pro publikování a odběry je řízen lokálními definicemi zabezpečení a pravidly, které jsou popsány v tématu [Zabezpečení publikování/odběru](#). V systému z/OS není pro zavedení řízení přístupu požadován žádný lokální objekt tématu. Pro řízení přístupu na jiných platformách není vyžadováno žádné lokální téma. Administrátoři se mohou rozhodnout použít řízení přístupu k objektům klastrovaných témat bez ohledu na to, zda již v klastru existují.

Systémoví administrátoři jsou odpovědní za řízení přístupu na svém lokálním systému. Musí důvěřovat administrátorům ostatních členů hierarchie nebo kolektivu klastru, aby byli odpovědní za jejich zásadu řízení přístupu. Vzhledem k tomu, že řízení přístupu je definováno pro každý samostatný počítač, je pravděpodobné, že bude tíživé, je-li zapotřebí kontrola na úrovni pokuty. Ve stromu témat nemusí být nutné definovat žádné řízení přístupu nebo řízení přístupu k vyšším objektům. Řízení přístupu na úrovni FGT lze definovat pro každou dílčí divizi oboru názvů témat.

### Vytvoření proxy odběru

Důvěryhodnost organizace pro připojení správce front k vašemu správci front je potvrzena běžnými prostředky ověřování kanálu. Je-li tato důvěryhodná organizace také povolena k distribuovanému publikování/odběru, provede se kontrola oprávnění. Kontrola se provede, když kanál vloží zprávu do fronty distribuovaných publikování/odběru. Je-li například vložena zpráva do fronty SYSTEM.INTER.QMGR.CONTROL. ID uživatele pro kontrolu oprávnění fronty závisí na hodnotách typu PUTAUT přijímajícího kanálu. Příklad: ID uživatele kanálu, MCAUSER, kontext zprávy, v závislosti na hodnotě a platformě. Další informace o zabezpečení kanálu naleznete v tématu [Zabezpečení kanálů](#).

Odběry proxy se provádějí s ID uživatele distribuovaného agenta publikování/odběru ve vzdáleném správci front. Například QM2 v [Obrázek 38 na stránce 102](#). Uživateli je poté snadno udělen přístup k lokálním profilům objektů tématu, protože ID uživatele je v systému definováno a neexistují tedy žádné konflikty domén.



Obrázek 38. Zabezpečení odběru proxy, provedení odběru

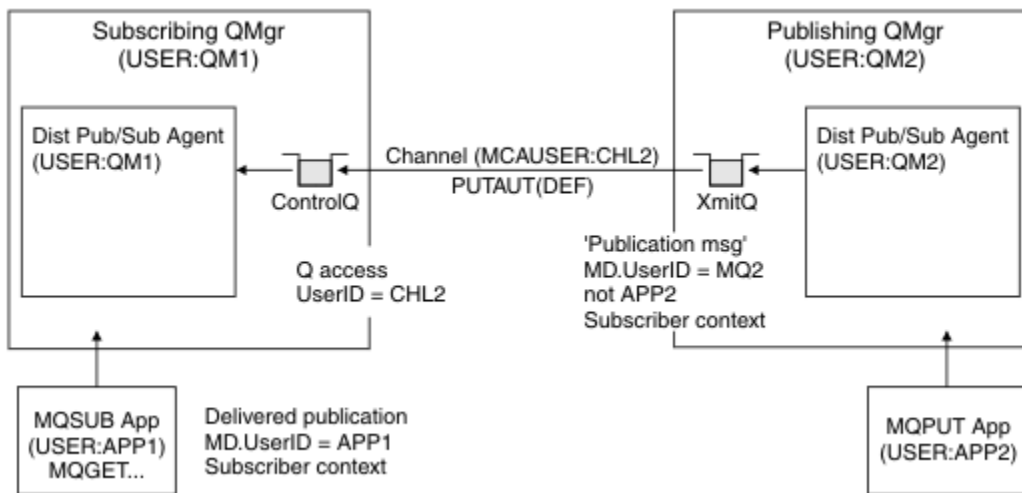
### Odeslání vzdálených publikování

Je-li publikace vytvořena ve správci front publikování, je vytvořena kopie publikování pro každý odběr proxy. Kontext zkopírované publikace obsahuje kontext ID uživatele, který vytvořil odběr; QM2 v produktu

Obrázek 39 na stránce 103. Proxy odběr se vytvoří s cílovou frontou, která je vzdálenou frontou, takže je zpráva publikování vyřešena do přenosové fronty.

Důvěryhodnost organizace pro připojení svého správce front QM2k jinému správci front QM1 je potvrzena normálním ověřováním kanálu. Je-li tato důvěryhodná organizace poté povolena pro distribuované publikování/odběr, provede se kontrola oprávnění, když kanál vloží zprávu publikování do fronty publikování distribuovaného publikování/odběru SYSTEM . INTER . QMGR . PUBS. ID uživatele pro kontrolu oprávnění fronty závisí na hodnotě parametru PUTAUT přijímajícího kanálu (například ID uživatele kanálu, MCAUSER, kontext zprávy a další informace v závislosti na hodnotě a platformě). Další informace o zabezpečení kanálu naleznete v tématu Zabezpečení kanálů.

Když se zpráva o publikování dostane do správce front odběru, provede se další příkaz MQPUT pro dané téma pod oprávněním správce front a kontext s touto zprávou je nahrazen kontextem každého z lokálních odběratelů, protože každá z nich má danou zprávu.



Obrázek 39. Zabezpečení odběru proxy, postoupení publikací

V systému, kde bylo zvažováno, že se týká zabezpečení, je pravděpodobné, že procesy distribuovaného publikování/odběru budou spuštěny pod ID uživatele ve skupině mqm , parametr MCAUSER na kanálu je prázdný (předvolba) a zprávy se doručí do různých systémových front podle potřeby. Nezabezpečený systém umožňuje snadné nastavení koncepce k demonstraci distribuovaného publikování/odběru.

V systému, kde je zabezpečení vážnější, se na tyto interní zprávy vztahují stejné ovládací prvky zabezpečení jako každá zpráva, která se přešla přes kanál.

Pokud je kanál nastaven s neprázdnou hodnotou MCAUSER a hodnotou PUTAUT určující, že MCAUSER musí být zkontrolována, pak musí mít MCAUSER udělen přístup k frontám SYSTEM . INTER . QMGR . \* . Existuje-li více různých vzdálených správců front s kanály spuštěnými pod různými identifikátory MCAUSER , je třeba všem těmto ID uživatelů udělit přístup k frontám produktu SYSTEM . INTER . QMGR . \* . Kanály spuštěné pod různými ID MCAUSER se mohou vyskytnout například v případě, že je v jednom správci front nakonfigurováno více hierarchických připojení.

Je-li kanál nastaven s hodnotou PUTAUT určující, že je použit kontext zprávy, pak je přístup k frontám SYSTEM . INTER . QMGR . \* kontrolován na základě ID uživatele uvnitř interní zprávy. Protože všechny tyto zprávy jsou vloženy s ID uživatele distribuovaného agenta publikování/odběru ze správce front, který odesílá interní zprávu, nebo zprávu publikování (viz Obrázek 39 na stránce 103), není příliš velká sada ID uživatelů pro udělení přístupu k různým systémovým frontám (jeden pro vzdáleného správce front), pokud chcete tímto způsobem nastavit zabezpečení distribuovaného publikování/odběru. Stále má všechny stejné problémy, které zabezpečení kontextu kanálu vždy má, a to z různých domén ID uživatele a skutečnost, že ID uživatele ve zprávě nemusí být definováno v přijímajícím systému. Je to však naprosto přijatelný způsob, jak se v případě potřeby spustit.

Všechny systémy zpráv mezi správci front pro účely distribuovaných publikování/odběru se spouštějí s použitím běžného zabezpečení kanálu.

Informace o omezení publikování a odběrů proxy na úrovni tématu naleznete v tématu [Zabezpečení publikování/odběru](#).

## Použití výchozích ID uživatelů s hierarchií správce front

Pokud máte hierarchii správců front spuštěných na různých platformách a používáte výchozí ID uživatelů, všimněte si, že tato výchozí ID uživatele se liší mezi platformami a nemusí být známá na cílové platformě. Výsledkem je, že správce front spuštěný na jedné platformě zamítá zprávy přijaté od správců front na jiných platformách s kódem příčiny MQRC\_NOT\_AUTHORIZED.

Chcete-li zabránit odmítnutí zpráv, je třeba přidat k výchozím ID uživatele, která se používají na jiných platformách, následující oprávnění:

- \*PUT \*GET oprávnění na SYSTEM.BROKER. fronty
- \*PUB \*SUB oprávnění na systému SYSTEM.BROKER. Témata
- \*ADMCR \*ADMDEL \*ADMCHG oprávnění na SYSTEM.BROKER.CONTROL.QUEUE fronta.

Výchozí ID uživatele jsou následující:

Platforma	Předvolené ID uživatele
Windows	MUSR_MQADMIN <b>Poznámka:</b> MUSR_MQADMIN je výchozí ID uživatele pouze pro první instalaci. V případě následných instalací vytvoří Průvodce přípravou produktu IBM WebSphere MQ uživatelský účet s názvem MUSR_MQADMINx, kde x je další dostupné číslo představující ID uživatele, které neexistuje.
Systémy UNIX and Linux	mqm
IBM i	QMQM
z/OS	ID uživatele adresního prostoru inicializátoru kanálu

Vytvořte a udělte přístup k ID uživatele 'qmqm', je-li hierarchicky připojen ke správci front v systému IBM i for Queue Managers na platformách Windows, UNIX, Linux a z/OS.

Vytvořte a udělte přístup k ID uživatele 'mqm', pokud je hierarchicky připojeno ke správci front v systémech Windows, UNIX nebo Linux for Queue Managers na platformách IBM i a z/OS.

Vytvořte a udělte uživateli přístup k ID uživatele adresního prostoru kanálu pro iniciátor kanálu z/OS, pokud je hierarchicky připojeno ke správci front v systému z/OS for Queue Manager na platformách Windows, UNIX, Linux a IBM i.

ID uživatelů mohou rozlišovat malá a velká písmena. Původní správce front (pokud systémy IBM i, Windows, UNIX nebo Linux) vynutí, aby ID uživatele bylo vše velkými písmeny. Přijímající správce front (pokud systémy Windows, UNIX nebo Linux) vynutí, aby ID uživatele bylo zadáno malými písmeny. Proto musí být všechna ID uživatelů vytvořená na systémech UNIX and Linux vytvořena ve svém formátu s malými písmeny. Byla-li instalována uživatelská procedura pro zprávy, vynucuje se ID uživatele velkými nebo malými písmeny. Je třeba věnovat pozornost tomu, jak procedura ukončení zprávy zpracovává ID uživatele.

Chcete-li se vyhnout potenciálním problémům s převodem ID uživatelů, postupujte takto:

- V systémech UNIX, Linux a Windows se ujistěte, že ID uživatelů jsou uvedena malými písmeny.
- V systémech IBM i a z/OS kontrolujte, zda jsou ID uživatelů zadána velkými písmeny.

### **Systemové fronty distribuovaného publikování/odběru**

Správce front pro systém zpráv publikování/odběru používají čtyři systémové fronty. Musíte si být vědomi své existence pouze pro účely určování problémů nebo plánování kapacity.



<i>Tabulka 9. Systémové fronty publikování/odběru na distribuovaných platformách</i>	
<b>Systémová fronta</b>	<b>Účel</b>
SYSTEM.INTER.QMGR.CONTROL	Řídící fronta distribuovaných publikování/odběru WebSphere MQ
SYSTEM.INTER.QMGR.FANREQ	WebSphere MQ distribuovaná interní proxy-výstupní fronta procesu pro odběr/odběr-out vstupní fronty
SYSTEM.INTER.QMGR.PUBS	Publikace distribuovaného publikování/odběru produktu WebSphere MQ
SYSTEM.HIERARCHY.STATE	WebSphere MQ -stav relace s distribuovanou hierarchií publikování/odběru

Atributy systémových front publikování/odběru jsou zobrazeny v [Tabulka 10](#) na stránce 105.

<i>Tabulka 10. Atributy front systému publikování/odběru</i>	
<b>Atribut</b>	<b>Výchozí hodnota</b>
DEFPSIST	Ano
DEFSOPT	V
MAXMSGL	Na platformách AIX, HP-UX, Linux, IBM i, Solaris a Windows : Hodnota parametru MAXMSGL příkazu ALTER QMGR.
MAXDEPTH	999999999
SHARE	Není k dispozici
STGCLASS	Tento atribut se používá pouze na platformách z/OS

#### *Chyby fronty systému publikování/odběru*

Chyby se mohou vyskytnout, když jsou distribuované fronty správce front publikování/odběru nedostupné.

Je-li fronta požadavků SYSTEM.INTER.QMGR.FANREQ je nedostupný, rozhraní MQSUB API přijímá kódy příčiny a chybové zprávy zapsané do protokolu chyb při příležitostech, kdy je třeba proxy odběry doručit přímo připojeným správcům front.

Pokud je ve frontě stavu relace hierarchie SYSTEM.HIERARCHY.STATE není k dispozici, chybová zpráva se запиše do protokolu chyb a generátor publikování/odběru se vloží do režimu COMPAT.

Pokud je některý z ostatních SYSTEM.INTER.QMGR jsou nedostupné, do protokolu chyb se запиše chybová zpráva a ačkoli funkce není zakázána, je pravděpodobné, že zprávy publikování/odběru budou sestavovat ve frontách ve vzdálených správcích front.

Je-li fronta přenosu k nadřizovanému, podřizovanému nebo publikačnímu správci front klastru nebo odběru, není k dispozici:

1. Rozhraní MQPUT API přijímá kódy příčiny a publikace nejsou doručeny.
2. Přijaté publikace mezi správci front se zálohují do vstupní fronty a následně jsou provedeny znovu, jsou-li umístěny do fronty nedoručených zpráv, je-li dosažena prahová hodnota vrácení.
3. Odběry proxy se zálohují do fronty požadavků výstupního větvení a následně se znovu pokusí umístit do fronty nedoručených zpráv, je-li dosažena prahová hodnota odvolání; v takovém případě nebude proxy odběr doručen do žádného připojeného správce front.
4. Zprávy protokolu relace hierarchie se nezdařily a stav připojení je v příkazu PUBSUB označen jako CHYBA.

## Práce s nedoručené zprávy s obslužnou rutinou fronty WebSphere MQ : Dead-letter

Co je fronta nedoručených zpráv, jak jsou na ní zprávy vloženy a jak ji lze spravovat?

*Fronta nedoručených zpráv* (DLQ), někdy označovaná jako *fronta nedoručených zpráv*, je zadržující fronta pro zprávy, které nelze doručit do cílových front. Každý správce front v síti by měl mít přidružený DLQ.

Zprávy lze vkládat do fronty DLQ správci front, agenty kanálů zpráv (MCA) a aplikací. Všechny zprávy na DLQ musí mít předponu ve struktuře *dead-letter header*, MQDLH.

Zprávy odeslané do fronty DLQ správcem front nebo agentem kanálu zpráv mají vždy MQDLH; aplikace, které předávají zprávy do fronty nedoručených zpráv, musí dodat rozhraní MQDLH. Pole *Příčina* struktury MQDLH obsahuje kód příčiny, který identifikuje důvod, proč se zpráva nachází na DLQ.

Všechna prostředí WebSphere MQ vyžadují rutinu pro pravidelné zpracování zpráv na frontě DLQ. Produkt WebSphere MQ poskytuje výchozí rutinu, která se nazývá *obslužná rutina fronty nedoručených zpráv* (obslužná rutina DLQ), kterou vyvoláte pomocí příkazu `runmqdlq`.

Instrukce pro zpracování zpráv na DLQ se dodávají do popisovače DLQ pomocí uživatelem napsaného *tabulky pravidel*. To znamená, že se obslužná rutina DLQ porovnává se zprávami na DLQ proti položkám v tabulce pravidel; když se zpráva DLQ shoduje s položkou v tabulce pravidel, obslužná rutina DLQ provede akci přidruženou k této položce.

### Vyvolání obslužné rutiny DLQ

Vyvolejte obslužnou rutinu DLQ pomocí příkazu `runmqdlq`. Název fronty DLQ, kterou chcete zpracovat, a správce front, který chcete použít, můžete pojmenovat dvěma způsoby.

Tyto dva způsoby jsou následující:

- Jako parametry příkazu `runmqdlq` z příkazového řádku. Příklad:

```
runmqdlq ABC1.DEAD.LETTER.QUEUE ABC1.QUEUE.MANAGER <qrule.rul
```

- V tabulce pravidel. Příklad:

```
INPUTQ(ABC1.DEAD.LETTER.QUEUE) INPUTQM(ABC1.QUEUE.MANAGER)
```

Příklady platí pro DLQ s názvem ABC1.DEAD.LETTER.QUEUE, kterou vlastní správce front ABC1.QUEUE.MANAGER.

Pokud nezádáte frontu nedoručených zpráv nebo správce front, bude použit výchozí správce front pro danou instalaci spolu s frontou DLQ náležícím do daného správce front.

Příkaz `runmqdlq` vezme svůj vstup z `stdin`; přidružíte tabulku pravidel k `runmqdlq` přesměrováním `stdin` z tabulky pravidel.

Chcete-li spustit obslužnou rutinu DLQ, musíte mít oprávnění k přístupu jak k samotnému DLQ, tak ke všem frontám zpráv, ke kterým se budou zprávy na DLQ předávat. Aby mohl program DLQ vkládat zprávy do front s oprávněním ID uživatele v kontextu zprávy, musíte mít také oprávnění k převzetí identity jiných uživatelů.

Další informace o příkazu `runmqdlq` naleznete v souboru [runmqdlq](#).

### Ukázkový popisovač DLQ, `amqsdlq`

Kromě obslužné rutiny DLQ vyvolané pomocí příkazu `runmqdlq` poskytuje produkt WebSphere MQ zdroj ukázkového manipulátoru DLQ, `amqsdlq`, s funkcí, která je podobná funkci, kterou poskytuje `runmqdlq`.

Můžete upravit parametr `amqsdlq` tak, aby poskytoval obslužnou rutinu DLQ, která splňuje vaše požadavky. Můžete se například rozhodnout, že chcete obslužnou rutinu DLQ, která může zpracovávat zprávy bez záhlaví zablokovaných písmen. (Oba výchozí obslužná rutina DLQ i ukázka, `amqsdlq`, zpracovávají pouze zprávy na DLQ, které začínají hlavičkou nedoručených zpráv, MQDLH. Zprávy, které

nezačínají rozhraním MQDLH, jsou identifikovány jako chybné a zůstávají na frontě DLQ po neomezenou dobu.)

`MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, do kterého je produkt WebSphere MQ nainstalován.

V produktu WebSphere MQ for Windows je zdroj `amqsdlq` zadán v adresáři:

```
MQ_INSTALLATION_PATH\tools\c\samples\dlq
```

a zkompilovaná verze se dodává v adresáři:

```
MQ_INSTALLATION_PATH\tools\c\samples\bin
```

V produktu WebSphere MQ pro systémy UNIX and Linux je zdroj `amqsdlq` zadán v adresáři:

```
MQ_INSTALLATION_PATH/samp/dlq
```

a zkompilovaná verze se dodává v adresáři:

```
MQ_INSTALLATION_PATH/samp/bin
```

## Tabulka pravidel obslužné rutiny DLQ

Tabulka pravidel obslužné rutiny DLQ definuje, jak obslužná rutina DLQ zpracovává zprávy, které dorazí do fronty DLQ.

V tabulce pravidel existují dva typy položek:

- První záznam v tabulce, který je volitelný, obsahuje *řídící data*.
- Všechny ostatní položky v tabulce jsou *pravidla* pro obslužnou rutinu DLQ, která se má sledovat. Každé pravidlo se skládá ze *vzorku* (sady charakteristik zprávy), proti kterému je zpráva porovnávána, a *akce*, která má být provedena, když se zpráva na DLQ shoduje se zadaným vzorem. V tabulce pravidel musí existovat alespoň jedno pravidlo.

Každá položka v tabulce pravidel se skládá z jednoho nebo více klíčových slov.

### Kontrolní údaje

Tato sekce popisuje klíčová slova, která můžete zahrnout do položky řídicí datové položky v tabulce pravidel obslužných rutin DLQ.

#### Poznámka:

- Svislá čára (|) odděluje alternativy, pouze jedna z nich může být uvedena.
- Všechna klíčová slova jsou volitelná.

#### INPUTQ (QueueName| '\_\_\_')

Název fronty DLQ, kterou chcete zpracovat:

1. Každá hodnota INPUTQ, kterou zadáte jako parametr do příkazu `runmqdlq`, potlačí všechny hodnoty INPUTQ v tabulce pravidel.
2. Pokud nezadáte hodnotu INPUTQ jako parametr příkazu `runmqdlq`, ale vy **do** zadáte hodnotu v tabulce pravidel, použije se hodnota INPUTQ v tabulce pravidel.
3. Není-li uveden žádný DLQ nebo uvedete INPUTQ ("") v tabulce pravidel, použije se název fronty DLQ patřící ke správci front s názvem, který je zadán jako parametr příkazu `runmqdlq`.
4. Pokud nezadáte hodnotu INPUTQ jako parametr příkazu `runmqdlq` nebo jako hodnotu v tabulce pravidel, použije se fronta DLQ patřící ke správci front uvedenému v klíčovém slově INPUTQM v tabulce pravidel.

#### INPUTQM (QueueManagerName| '\_\_\_')

Název správce front, který vlastní fronty DLQ pojmenované podle klíčového slova INPUTQ:

1. Každá hodnota INPUTQM, kterou zadáte jako parametr do příkazu `runmqdlq`, potlačí všechny hodnoty INPUTQM v tabulce pravidel.
2. Pokud do příkazu `runmqdlq` nezadáte hodnotu INPUTQM jako parametr, použije se hodnota INPUTQM v tabulce pravidel.
3. Není-li zadán správce front nebo v tabulce pravidel uvedete INPUTQM (""), použije se výchozí správce front pro danou instalaci.

#### **RETRYINT (Interval|\_60)**

Interval, v sekundách, kdy má obslužná rutina DLQ znovu zpracovat zprávy na DLQ, který nemohl být zpracován při prvním pokusu, a pro které byly požadovány opakované pokusy. Ve výchozím nastavení je interval opakování 60 sekund.

#### **WAIT (YES| NO |nnn)**

Zda má obslužná rutina DLQ čekat na příchod dalších zpráv do fronty DLQ, když zjistí, že neexistují žádné další zprávy, které by mohl zpracovat.

##### **YES**

Obslužná rutina DLQ čeká nekonečně dlouhou dobu.

##### **NO**

Obslužná rutina DLQ končí, když zjistí, že fronta DLQ je buď prázdná, nebo neobsahuje žádné zprávy, které by mohl zpracovat.

##### **nnn**

Obslužná rutina DLQ čeká na *nnn* sekund, než se nová práce objeví před ukončením, poté, co zjistí, že je fronta prázdná nebo neobsahuje žádné zprávy, které by mohl zpracovat.

Zadejte WAIT (YES) pro zaneprázdněné fronty DLQ a WAIT (NO) nebo WAIT (*nnn*) pro fronty nedoručených zpráv, které mají nízkou úroveň aktivity. Je-li obslužná rutina DLQ povolena pro ukončení, vyvolejte ji znovu s použitím spouštěče. Další informace o spouštění naleznete v tématu [Spuštění aplikací produktu WebSphere MQ pomocí spouštěčů](#).

Alternativou k zahrnutí řídicích dat do tabulky pravidel je dodat názvy fronty nedoručených zpráv a příslušného správce front jako vstupní parametry příkazu `runmqdlq`. Uvedete-li hodnotu v tabulce pravidel i jako vstup příkazu `runmqdlq`, má přednost hodnota zadaná v příkazu `runmqdlq`.

Pokud zahrnete do tabulky pravidel záznam řídicích dat, musí se jednat o **první** položku v tabulce.

#### **Pravidla (vzory a akce)**

Popis klíčových slov odpovídajících vzoru (ty, proti nimž jsou zprávy na DLQ porovnávány), a klíčová slova akce (ty, které určují, jak se má obslužná rutina DLQ zpracovat odpovídající zprávy). K dispozici je také ukázkové pravidlo.

#### **Klíčová slova pattern-matching**

Klíčová slova pattern-matching, která slouží k určení hodnot, se kterými se budou zprávy shodovat se zprávami v DLQ, jsou následující. (Všechna klíčová slova odpovídající vzoru jsou volitelná):

##### **APPLIDAT (ApplIdentityData|\_\*)**

Hodnota *ApplIdentityData* uvedená v deskriptoru zpráv MQMD zprávy na DLQ.

##### **APPLNAME (PutApplNázev|\_\*)**

Název aplikace, která vydala volání MQPUT nebo MQPUT1, jak je uvedeno v poli *PutApplName* deskriptoru zpráv MQMD, zprávy na DLQ.

##### **APPLTYPE (PutApplTyp|\_\*)**

Hodnota *PutApplType*, uvedená v deskriptoru zpráv MQMD, zprávy na DLQ.

##### **DESTQ (QueueName|\_\*)**

Název fronty zpráv, pro kterou je zpráva určena.

##### **DESTQM (QueueManagerName|\_\*)**

Název správce fronty fronty zpráv, pro který je zpráva určena.

**FEEDBACK (Zpětná vazba|\_\*)**

Je-li hodnota *MsgType* hodnotou MQFB\_REPORT, popisuje *Váš názor* povahu sestavy.

Symbolické názvy můžete používat. Například můžete použít symbolický název MQFB\_COA k identifikaci těchto zpráv na frontě nedoručených zpráv, které potřebují potvrzení o svém příchodu do cílových front.

**FORMAT (Formát|\_\*)**

Název, který odesílatel zprávy používá k popisu formátu dat zprávy.

**MSGTYPE (MsgType|\_\*)**

Typ zprávy na DLQ.

Symbolické názvy můžete používat. Například můžete použít symbolický název MQMT\_REQUEST k identifikaci těch zpráv na DLQ, které potřebují odpovědi.

**PERSIST (Perzistence|\_\*)**

Hodnota perzistence zprávy. (Trvalost zprávy určuje, zda přežije restarty správce front.)

Symbolické názvy můžete používat. Například můžete použít symbolický název MQPER\_PERSISTENT k identifikaci zpráv na DLQ, které jsou trvalé.

**REASON (ReasonCode|\_\*)**

Kód příčiny, který popisuje, proč byla zpráva vložena do fronty DLQ.

Symbolické názvy můžete používat. Například můžete použít symbolický název MQRC\_Q\_FULL k identifikaci těch zpráv umístěných na DLQ, protože jejich cílové fronty byly plné.

**REPLYQ (QueueName|\_\*)**

Název fronty pro odpověď určený v deskriptoru zprávy MQMD, zprávy v protokolu DLQ.

**REPLYQM (QueueManagerName|\_\*)**

Název správce front pro frontu odpovědí, určený v deskriptoru zpráv MQMD, zprávy v protokolu DLQ.

**USERID (UserIdentifier|\_\*)**

ID uživatele, který vytvořil zprávu na DLQ, jak je uvedeno v deskriptoru zpráv, MQMD, zprávy na DLQ.

**Klíčová slova akce**

Klíčová slova akcí, která se používá k popisu, jak se má zpracovat odpovídající zpráva, jsou následující:

**AKCE (DISCARD|IGNORE|RETRY|FWD)**

Akce, která má být provedena pro každou zprávu na DLQ, která odpovídá vzoru definovanému v tomto pravidle.

**Zahodit**

Vymažte zprávu z DLQ.

**IGNORE**

Nechte zprávu na DLQ.

**RETRY**

Pokud se první pokus o vložení zprávy do cílové fronty nezdaří, zkuste to znovu. Klíčové slovo RETRY nastaví počet pokusů provedených k implementaci akce. Klíčové slovo RETRYINT řídících dat řídí interval mezi pokusy.

**VPŘED**

Přeposlat zprávu do fronty uvedené v klíčovém slově FWDQ.

Je třeba určit klíčové slovo ACTION.

**FWDQ (QueueName| & DESTQ | & REPLYQ)**

Název fronty zpráv, do které má být postoupána zpráva, když je požadována akce ACTION (FWD).

**QueueName**

Název fronty zpráv. FWDQ (") není platný.

**& DESTQ**

Do pole *DestQName* ve struktuře MQDLH zadejte název fronty.

### **& REPLYQ**

Použijte název fronty z pole *ReplyToQ* v deskriptoru zpráv, MQMD.

Chcete-li se vyvarovat chybových zpráv, když pravidlo uvádějící FWDQ (& REPLYQ) odpovídá zprávě s prázdným polem *ReplyToQ*, uveďte REPLYQ (? \*) ve vzoru zprávy.

### **FWDQM (QueueManagerName| & DESTQM | & REPLYQM | '\_\_\_')**

Správce front pro frontu, do níž má být odeslána zpráva.

#### **QueueManagerNázev**

Název správce front pro frontu, do níž má být přesměrována zpráva, když je požadována akce ACTION (FWD).

### **& DESTQM**

V poli MQDLH použijte název správce front z pole *NázevDestQMgr*.

### **& REPLYQM**

Odeberte název správce front z pole *ReplyToQMgr* v deskriptoru zpráv, MQMD.

''

FWDQM (''), což je výchozí hodnota, identifikuje lokálního správce front.

### **ZÁHLAVÍ (YES| NE)**

Zda by měl příkaz MQDLH zůstat na zprávě, pro kterou je požadována akce ACTION (FWD). Ve výchozím nastavení zůstává MQDLH na zprávě. Klíčové slovo HEADER není platné pro akce jiné než FWD.

### **PUTAUT (DEF| CTX)**

Oprávnění, které má být programem DLQ uvedena do zpráv:

#### **DEF**

Vložte zprávy s oprávněním samotné obslužné rutiny DLQ.

#### **CTX**

Vložte zprávy s oprávněním ID uživatele do kontextu zprávy. Zadáte-li PUTAUT (CTX), musíte mít autorizaci k převzetí identity jiných uživatelů.

### **RETRY (RetryCount| \_1)**

Počet pokusů akce v rozsahu 1-999 999 999 k provedení akce (v intervalu uvedeném v klíčovém slově RETRYINT řídicích dat). Počet pokusů učiněných manipulátorem DLQ při implementaci jakéhokoli konkrétního pravidla je specifický pro aktuální instanci obslužné rutiny DLQ; tento počet netrvá po restartu. Je-li obslužná rutina DLQ restartována, počet pokusů provedených k použití pravidla je resetován na nulu.

## **Ukázkové pravidlo**

Zde je příklad pravidla z tabulky pravidel pro obslužné rutiny DLQ:

```
PERSIST(MQPER_PERSISTENT) REASON (MQRC_PUT_INHIBITED) +  
ACTION (RETRY) RETRY (3)
```

Toto pravidlo dává obslužnému programu DLQ pokyn k provedení tří pokusů doručit do cílové fronty trvalou zprávu, která byla vložena do fronty DLQ, protože MQPUT a MQPUT1 byly zablokovány.

Všechna klíčová slova, která můžete použít na pravidle, jsou popsána ve zbývající části této sekce. Všimněte si následujícího:

- Je-li nějaká hodnota klíčové slovo, je podtržena výchozí hodnota klíčového slova. Pro většinu klíčových slov je výchozí hodnota \* (hvězdička), která odpovídá libovolné hodnotě.
- Svislá čára (|) odděluje alternativy, pouze jedna z nich může být uvedena.
- Všechna klíčová slova kromě ACTION jsou volitelná.

### **Konvence pro tabulku pravidel**

Syntaxe, struktura a obsah tabulky pravidel obslužných rutin DLQ musí odpovídat těmto konvencím.

Tabulka pravidel musí dodržovat následující konvence:

- Tabulka pravidel musí obsahovat alespoň jedno pravidlo.
- Klíčová slova se mohou vyskytnout v libovolném pořadí.
- Klíčové slovo může být zahrnuto pouze jednou v jakémkoli pravidle.
- Klíčová slova nerozlišují velká a malá písmena.
- Klíčové slovo a jeho hodnota parametru musí být odděleny od jiných klíčových slov alespoň jednou mezerou nebo čárkou.
- Na začátku nebo na konci pravidla může být libovolný počet mezer a mezi klíčovými slovy, interpunkčním znaménkem a hodnotami.
- Každé pravidlo musí začínat na novém řádku.
- Na systémech Windows musí poslední pravidlo v tabulce končit znakem znaku návrat na začátek řádku/LF. Toho můžete dosáhnout tím, že zajistíte, že stisknete klávesu Enter na konci pravidla, takže poslední řádek tabulky je prázdný řádek.
- Z důvodů přenositelnosti nesmí být významná délka řádku větší než 72 znaků.
- Znak plus (+) použijte jako poslední neprázdný znak na řádku, abyste indikovali, že pravidlo pokračuje od prvního nemezerových znaků na dalším řádku. Znak minus (-) použijte jako poslední neprázdný znak na řádku, abyste indikovali, že pravidlo bude pokračovat od začátku dalšího řádku. V klíčových slovech a parametrech se mohou vyskytnout následující znaky.

Příklad:

```
APPLNAME(' ABC+  
D')
```

má za následek "ABCD" a

```
APPLNAME(' ABC-  
D')
```

bude mít za následek ' ABC D'.

- Řádky s komentářem, které začínají hvězdičkou (\*), se mohou vyskytovat kdekoli v tabulce pravidel.
- Prázdné řádky se ignorují.
- Každá položka v tabulce pravidel obslužných rutin DLQ obsahuje jedno nebo více klíčových slov a jejich přidružených parametrů. Parametry musí dodržovat následující pravidla syntaxe:
  - Každá hodnota parametru musí obsahovat alespoň jeden významný znak. Vymezení jednoduchých uvozovek v hodnotách, které jsou uzavřeny v uvozovkách, se nepovažují za významné. Tyto parametry jsou například platné:

FORMAT(' ABC ')	3 významné znaky
FORMAT(ABC)	3 významné znaky
FORMAT(' A ')	1 významný znak
FORMAT(A)	1 významný znak
FORMAT(' ')	1 významný znak

Tyto parametry jsou neplatné, protože neobsahují žádné významné znaky:

```
FORMAT(' ' )  
FORMAT( )  
FORMAT()  
FORMAT
```

- Jsou podporovány zástupné znaky. Otazník (?) můžete použít místo libovolného jediného znaku kromě koncové mezery; můžete použít hvězdičku (\*) místo nula nebo více sousedních znaků. Hvězdička (\*) a otazník (?) jsou **vždy** interpretovány jako zástupné znaky v hodnotách parametru.
- Zástupné znaky nelze zahrnout do parametrů těchto klíčových slov: ACTION, HEADER, RETRY, FWDQ, FWDQM a PUTAUT.
- Koncové mezery v hodnotách parametrů a v odpovídajících polích ve zprávě na DLQ nejsou významné, když se používají zástupné znaky. Avšak úvodní a vložené mezery v řetězcích, které jsou uzavřeny v jednoduchých uvozovkách, jsou významné pro shodu se zástupnými znaky.
- Numerické parametry nemohou obsahovat zástupný znak otazník (?). Můžete použít hvězdičku (\*) místo celého číselného parametru, ale ne jako část numerického parametru. Jedná se například o platné číselné parametry:

MSGTYPE(2)	Způsobilé jsou pouze zprávy odpovědí
MSGTYPE(*)	Jakýkoli typ zprávy je vhodný
MSGTYPE(' * ')	Jakýkoli typ zprávy je vhodný

Avšak MSGTYPE(' 2\* ') není platné, protože obsahuje hvězdičku (\*) jako část numerického parametru.

- Numerické parametry musí být v rozsahu 0-999 999 999. Je-li hodnota parametru v tomto rozsahu, je přijata, i když momentálně není platná v poli, ke kterému se klíčové slovo vztahuje. Pro číselné parametry můžete použít symbolické názvy.
- Je-li řetězcová hodnota kratší než pole v MQDLH nebo MQMD, ke kterému se klíčové slovo vztahuje, hodnota je vyplněna mezerami do délky pole. Je-li hodnota, kromě hvězdiček, delší než hodnota pole, je diagnostikována chyba. Například, jsou to všechny platné hodnoty řetězce pro 8znakové pole:

' ABCDEFGH '	8 znaků
' A*C*E*G*I '	5 znaků bez hvězdiček
' *A*C*E*G*I*K*M*O * '	8 znaků bez hvězdiček

- Uzavřete řetězce, které obsahují mezery, malé znaky nebo speciální znaky jiné než tečka (.), lomítko (?), podtržítka (\_) a znak procenta (%) v jednoduchých uvozovkách. Znaky malých písmen, které nejsou uzavřeny v jednoduchých uvozovkách, jsou složeny na velká písmena. Pokud řetězec obsahuje uvozovku, použijte dvě jednoduché uvozovky k označení začátku i konce cenové nabídky. Při výpočtu délky řetězce se každý výskyt dvojitých uvozovek považuje za jediný znak.

## Jak se zpracovává tabulka pravidel

Obslužná rutina fronty DLQ prohledá tabulku pravidel a hledá pravidlo, kde se vzorek shoduje se zprávou na DLQ.

Vyhledávání začne s prvním pravidlem v tabulce a pokračuje se sekvenčně přes tabulku. Když obslužná rutina DLQ najde pravidlo s odpovídajícím vzorem, převezme akci z tohoto pravidla. Obslužná rutina DLQ zvýší počet opakovaných pokusů pro pravidlo o 1 pokaždé, když použije toto pravidlo. Pokud se první pokus nezdaří, pokusí se obslužná rutina DLQ znovu zkusit, dokud se počet pokusů neshoduje s číslem uvedeným v klíčovém slově RETRY. Selže-li všechny pokusy, obslužná rutina DLQ vyhledá další porovnávací pravidlo v tabulce.

Tento proces se opakuje pro následná odpovídající pravidla, dokud nebude akce úspěšná. Když se každé vyhovující pravidlo pokusilo o počet pokusů, které byly uvedeny u klíčového slova RETRY, a všechny pokusy se nezdařily, předpokládá se ACTION (IGNORE). AKCE (IGNORE) se také předpokládá, pokud není nalezeno žádné vyhovující pravidlo.

### Poznámka:



1. Odpovídající vzory pravidel se hledají pouze pro zprávy na DLQ, které začínají na MQDLH. Zprávy, které nezačínají na MQDLH, jsou vykazovány pravidelně jako chybné a zůstávají na frontě DLQ po neomezenou dobu.
2. Všechna klíčová slova vzoru mohou být povolena jako výchozí, taková, že se pravidlo může skládat pouze z akce. Všimněte si však, že tato pravidla jsou použita pouze pro všechny zprávy ve frontě, které mají příkazy MQDLHs a které dosud nebyly zpracovány v souladu s ostatními pravidly v tabulce.
3. Tabulka pravidel se ověřuje, když se spustí obslužná rutina DLQ, a chyby jsou v této době označeny příznakem. Tabulka pravidel můžete kdykoli změnit, ale tyto změny se neprojeví, dokud se nerestartuje obslužná rutina DLQ.
4. Obslužná rutina DLQ nemění obsah zpráv, MQDLH ani deskriptor zprávy. Obslužná rutina DLQ vždy vloží zprávy do jiných front s volbou zprávy MQPMO\_PASS\_ALL\_CONTEXT.
5. Následné chyby syntaxe v tabulce pravidel nemusí být rozpoznány, protože tabulka pravidel je navržena tak, aby eliminovala generování opakovaných chyb během ověření platnosti.
6. Obslužná rutina DLQ otevře volbu DLQ s volbou MQOO\_INPUT\_AS\_Q\_DEF.
7. Několik instancí obslužné rutiny DLQ může běžet souběžně proti stejné frontě, a to pomocí stejné tabulky pravidel. Je však spíše obvyklé, že existuje vztah typu jeden-na-jeden mezi dvěma DLQ a ovladačem DLQ.

### **Zajištění toho, aby byly zpracovány všechny zprávy DLQ**

Obslužná rutina DLQ udržuje záznam o všech zprávách na DLQ, které byly zobrazeny, ale nebyly odebrány.

Pokud použijete obslužnou rutinu DLQ jako filtr pro extrakci malé podmnožiny zpráv z DLQ, obslužná rutina DLQ stále musí uchovat záznam těchto zpráv na DLQ, který nezpracoval. Obslužná rutina DLQ také nemůže zaručit, že budou zobrazeny nové zprávy přicházející do fronty DLQ, a to i v případě, že je fronta DLQ definovaná jako FIFO (first-in-first-out). Není-li fronta prázdná, je fronta DLQ pravidelně znovu skenována, aby kontrolovala všechny zprávy.

Z těchto důvodů se snažte zajistit, aby program DLQ obsahoval co nejméně zpráv; pokud zprávy, které nelze vyřadit nebo předány jiným frontám (z jakéhokoli důvodu), se mohou hromadit ve frontě, vytížení obslužné rutiny DLQ se zvýší a samotný DLQ se může zaplnit.

Můžete přijmout specifická opatření, která umožní programu DLQ prázdné fronty DLQ. Zkuste například použít volbu ACTION (IGNORE), která ponechá zprávy na DLQ zprávy. (Nezapomeňte, že hodnota ACTION (IGNORE) se předpokládá u zpráv, které nejsou explicitně adresovány jinými pravidly v tabulce.) Místo toho pro tyto zprávy, které byste jinak ignorovali, použijte akci, která přesune zprávy do jiné fronty. Příklad:

```
ACTION (FWD) FWDQ (IGNORED.DEAD.QUEUE) HEADER (YES)
```

Podobně platí, že poslední pravidlo v tabulce bude catchAll ke zpracování zpráv, které nebyly adresovány dřívějšími pravidly v tabulce. Konečné pravidlo v tabulce může být například něco podobného:

```
ACTION (FWD) FWDQ (REALLY.DEAD.QUEUE) HEADER (YES)
```

To předává zprávy, které spadají do konečného pravidla v tabulce do fronty REALLY.DEAD.QUEUE, kde je lze zpracovat ručně. Pokud takové pravidlo nemáte, zprávy pravděpodobně zůstanou na frontě DLQ po neomezenou dobu.

### **Příklad tabulky pravidel obslužných rutin DLQ**

Ukázková tabulka pravidel pro příkaz runmqdlq obsahující jednu položku řídicího prvku-data a několik pravidel.

```
*****
*           An example rules table for the runmqdlq command           *
*****
* Control data entry
* -----
* If no queue manager name is supplied as an explicit parameter to
```

```

* runmqdlq, use the default queue manager for the machine.
* If no queue name is supplied as an explicit parameter to runmqdlq,
* use the DLQ defined for the local queue manager.
*
inputqm(' ') inputq(' ')

* Rules
* -----
* We include rules with ACTION (RETRY) first to try to
* deliver the message to the intended destination.
* If a message is placed on the DLQ because its destination
* queue is full, attempt to forward the message to its
* destination queue. Make 5 attempts at approximately
* 60-second intervals (the default value for RETRYINT).

REASON(MQRC_Q_FULL) ACTION(RETRY) RETRY(5)

* If a message is placed on the DLQ because of a put inhibited
* condition, attempt to forward the message to its
* destination queue. Make 5 attempts at approximately
* 60-second intervals (the default value for RETRYINT).

REASON(MQRC_PUT_INHIBITED) ACTION(RETRY) RETRY(5)

* The AAAA corporation are always sending messages with incorrect
* addresses. When we find a request from the AAAA corporation,
* we return it to the DLQ (DEADQ) of the reply-to queue manager
* (&REPLYQM).
* The AAAA DLQ handler attempts to redirect the message.

MSGTYPE(MQMT_REQUEST) REPLYQM(AAAA.*) +
  ACTION(FWD) FWDQ(DEADQ) FWDQM(&REPLYQM)

* The BBBB corporation never do things by half measures. If
* the queue manager BBBB.1 is unavailable, try to
* send the message to BBBB.2

DESTQM(bbbb.1) +
  action(fwd) fwdq(&DESTQ) fwdqm(bbbb.2) header(no)

* The CCCC corporation considers itself very security
* conscious, and believes that none of its messages
* will ever end up on one of our DLQs.
* Whenever we see a message from a CCCC queue manager on our
* DLQ, we send it to a special destination in the CCCC organization
* where the problem is investigated.

REPLYQM(CCCC.*) +
  ACTION(FWD) FWDQ(ALARM) FWDQM(CCCC.SYSTEM)

```

```

* Messages that are not persistent run the risk of being
* lost when a queue manager terminates. If an application
* is sending nonpersistent messages, it should be able
* to cope with the message being lost, so we can afford to
* discard the message. PERSIST(MQPER_NOT_PERSISTENT) ACTION(DISCARD)
* For performance and efficiency reasons, we like to keep
* the number of messages on the DLQ small.
* If we receive a message that has not been processed by
* an earlier rule in the table, we assume that it
* requires manual intervention to resolve the problem.
* Some problems are best solved at the node where the
* problem was detected, and others are best solved where
* the message originated. We don't have the message origin,
* but we can use the REPLYQM to identify a node that has
* some interest in this message.
* Attempt to put the message onto a manual intervention
* queue at the appropriate node. If this fails,
* put the message on the manual intervention queue at
* this node.

REPLYQM('?*') +
  ACTION(FWD) FWDQ(DEADQ.MANUAL.INTERVENTION) FWDQM(&REPLYQM)

ACTION(FWD) FWDQ(DEADQ.MANUAL.INTERVENTION)

```

## Více instalací

---

V systému UNIX, Linux, and Windows je možné mít v systému více než jednu kopii produktu IBM WebSphere MQ .

Můžete zvolit, kde má být nainstalována každá kopie produktu IBM WebSphere MQ , ale každá kopie musí být v odděleném umístění instalace. Na jednom počítači může v daném okamžiku existovat maximálně 128 instalací produktu IBM WebSphere MQ . Jedna instalace může být instalací produktu IBM WebSphere MQ Version 7.0.1 v opravné sadě 6 nebo novější. Nyní máte na výběr:

- Udržet jednoduchost údržby a správy jedné instalace produktu IBM WebSphere MQ na počítači.
- Využijte výhod nabízených možností podpory více instalací produktu IBM WebSphere MQ .

Než nainstalujete více kopií produktu IBM WebSphere MQ , musíte provést několik rozhodnutí:

- Budete mít v systému kopii produktu IBM WebSphere MQ Version 7.0.1 ?

Je-li v systému nainstalován produkt IBM WebSphere MQ Version 7.0.1 s opravnou sadou 6 nebo novější, existuje řada omezení, která je třeba vzít v úvahu:

- Na systémech UNIX and Linux musí být produkt IBM WebSphere MQ Version 7.0.1 nainstalován ve výchozím umístění.
- IBM WebSphere MQ Version 7.0.1 musí být první instalací na systému. Produkt IBM WebSphere MQ Version 7.0.1 nemůžete instalovat po instalaci verze 7.1 nebo novější. Pokud odinstalujete verzi 7.0.1, nelze ji znovu instalovat, je-li nainstalována novější verze produktu WebSphere MQ .
- IBM WebSphere MQ Version 7.0.1 je automaticky primární instalací. Po instalaci produktu IBM WebSphere MQ Version 7.0.1 nemůžete vybrat jinou instalaci jako primární instalaci.

- Kam budete instalovat každou kopii produktu IBM WebSphere MQ?

Můžete zvolit umístění instalace pro vaše instalace ve verzi 7.1 nebo novější. Další informace naleznete v tématu [Výběr umístění instalace](#).

- Potřebujete primární instalaci?

Primární instalace je instalací, ke které se vztahují umístění v celém systému. Další informace viz téma [“Výběr primární instalace”](#) na stránce 116.

- Jak se budou vaše aplikace připojovat?

Měli byste zvážit, jak aplikace vyhledají odpovídající knihovny IBM WebSphere MQ . Další informace viz [Připojování aplikací v prostředí s více instalačními programy](#) a [Připojení aplikací .NET v prostředí s více instalačními prostředí](#).

- Je třeba změnit stávající východy?

Není-li produkt IBM WebSphere MQ nainstalován ve výchozím umístění, je třeba aktualizovat své uživatelské procedury. Další informace viz [Psaní a kompilace ukončení a instalovatelných služeb](#) .

- Který správce front bude přidružen k této instalaci?

Každý správce front je přidružen ke konkrétní instalaci. Instalace, ke které je správce front přidružen, omezuje správce front tak, aby mohl být spravován pouze příkazy z této instalace. Další informace naleznete v tématu [Přidružení správce front k instalaci](#).

- Jak nastavíte své prostředí pro práci s každou instalací?

Při použití více instalací v systému je třeba zvážit, jak budete pracovat s konkrétními instalacemi, a jak budete vydávat příkazy z této instalace. Buď můžete zadat úplnou cestu k příkazu, nebo můžete použít příkaz **setmqenv** nebo **crtmqenv** k nastavení proměnných prostředí. Nastavení proměnných prostředí vám umožňuje vynechat cestu k příkazům pro tuto instalaci. Další informace viz [setmqenv](#) a [crtmqenv](#).

Když jste odpověděli na tyto otázky, můžete produkt IBM WebSphere MQ nainstalovat pomocí kroků uvedených v tématu [Instalace produktu IBM WebSphere MQ](#).

Pokud máte existující instalace produktu IBM WebSphere MQ a chcete použít více možností instalace pro migraci z jedné verze produktu IBM WebSphere MQ na jinou verzi, přečtěte si téma [Koexistence správce front s více instalacemi v produktu UNIX, Linuxu a Windows](#).

## Klient služby IBM Message Service pro balík podpory .NET a vícenásobné instalace

Pro podporu více verzí musí být funkce *Java a .NET Messaging and Web Services* instalována spolu s produktem IBM WebSphere MQ. Tato funkce obsahuje všechny funkce obsažené v podpůrném balíku *IBM Message Service Client for .NET (IA9H)*. Je-li v systému nainstalován balík podpory, více verzí není podporováno. Před instalací produktu IBM WebSphere MQ musíte odinstalovat balík podpory. Další informace o instalaci funkce .NET naleznete v tématu [Instalace tříd produktu WebSphere MQ pro prostředí .NET](#).

### Související pojmy

[UNIX, Linux a Windows: Migrace na straně druhé strany z verze 7.0.1 na verzi 7.5](#)

[UNIX, Linux, a Windows: Migrace více fází z verze 7.0.1 na verzi 7.5](#)

### Související úlohy

[Konfigurace více instalací](#)

[Vyhledávání instalací produktu WebSphere MQ v systému](#)

## Výběr primární instalace

V systémech, které podporují více instalací produktu IBM WebSphere MQ (UNIX, Linux, and Windows), je primární instalací taková primární instalace, na kterou odkazují umístění v celém systému IBM WebSphere MQ. Primární instalace je volitelná, ale vhodná.

Před produktem IBM WebSphere MQ Version 7.1 může být v libovolném okamžiku nainstalována pouze jedna instance produktu. Na systémech Windows bylo několik globálních proměnných prostředí nastaveno tak, aby ukazovaly na tuto instalaci. Na systémech UNIX and Linux byly přidány symbolické odkazy do `/usr/lib`, `/usr/bin` a `/usr/include` ukazovaly na tuto jednoduchou instalaci.

V produktu Version 7.1 můžete v produktu UNIX, Linux, and Windows nainstalovat více verzí produktu IBM WebSphere MQ. Na jednom z těchto systémů můžete mít více než jednu instalaci produktu IBM WebSphere MQ na jednom z těchto systémů a volitelně můžete nakonfigurovat jednu z těchto instalací jako primární instalaci. Proměnné prostředí a symbolické odkazy ukazující na jednu instalaci jsou méně významné, když existuje více verzí. Některé funkce však vyžadují, aby tato umístění v rámci celého systému fungovala. Příklad: Vlastní uživatelské skripty pro administraci produktu IBM WebSphere MQ a produkty třetích stran. Tyto funkce fungují pouze na primární instalaci.

Pokud v systémech UNIX and Linux nastavíte instalaci jako primární instalaci, symbolické odkazy na externí knihovny a řídicí příkazy této instalace se přidají do produktů `/usr/lib` a `/usr/bin`. Nemáte-li primární instalaci, symbolické odkazy se nevytvoří. Seznam symbolických odkazů, které jsou provedeny v primární instalaci, najdete v tématu [Externí knihovna a příkaz pro řízení připojení k primární instalaci v systému UNIX and Linux](#).

Na systémech Windows se globální proměnné prostředí ukazují na adresáře, do kterých byla nainstalována primární instalace. Tyto proměnné prostředí se používají k vyhledání knihoven produktu IBM WebSphere MQ, řídicích příkazů a souborů záhlaví. Kromě toho v systémech Windows vyžadují některé funkce operačního systému centrální registraci knihoven rozhraní, které jsou poté načteny do jednoho procesu. V případě více verzí produktu IBM WebSphere MQ budou existovat konfliktní sady knihoven IBM WebSphere MQ. Funkce se pokusí načíst tyto konfliktní sady knihoven do jednoho procesu. Proto mohou být takové funkce použity pouze s primární instalací. Podrobnosti o některých funkcích, které jsou omezené na použití s primární instalací, viz [Funkce, které lze použít pouze s primární instalací v systému Windows](#).

Máte-li v systému instalaci produktu IBM WebSphere MQ Version 7.0.1, je tato instalace automaticky primární instalací. Primární instalaci nelze změnit, je-li nainstalován produkt Version 7.0.1. Pokud jsou všechny instalace v systému Version 7.1 nebo novější, můžete zvolit, zda se má mít primární instalace. Zvažte volby v produktu [Tabulka 11 na stránce 117](#).

Tabulka 11. Volby primární instalace.

Tato tabulka obsahuje platné konfigurace instalace pro primární instalace. S jediným produktem Version 7.1nebo novějším může být buď primární, nebo nepřímá. S více instalacemi, jedním z Version 7.0.1 a jedním nebo více v Version 7.1nebo novějším, musí být primární serverVersion 7.0.1 primární a ostatní instalace musí být nepřímá. S více instalacemi v produktu Version 7.1nebo novějším může být jedna instalace primární, nebo všechny instalace nemohou být primární.

Volby	Platné konfigurace instalace		Další informace
	Primární	Nepřímá	
Samostatná instalace produktu Version 7.1nebo novější.	Version 7.1nebo novější	Není	Chcete-li pokračovat v práci s jednou instalací stejným způsobem jako předchozí vydání, nakonfigurujte instalaci jako primární instalaci. Informace o této volbě naleznete v tématu <a href="#">Jediná instalace produktu IBM WebSphere MQ Version 7.1nebo novější, konfigurovaná jako primární instalace</a> .
	Není	Version 7.1nebo novější.	Chcete-li pokračovat v práci s jednou instalací, ale nechcete vytvořit symbolické odkazy nebo globální proměnné prostředí vytvořené pro vás, nakonfigurujte instalaci jako nepřímá. Informace o důsledcích této volby naleznete v tématu <a href="#">Jedna instalace produktu IBM WebSphere MQ Version 7.1nebo novější, nakonfigurovaná jako nepřímá</a> .
Více instalací: Version 7.0.1 a Version 7.1nebo novější.	Version 7.0.1	Version 7.1nebo novější.	Chcete-li mít více instalací produktu IBM WebSphere MQ, s verzí 7.0.1, je instalace verze 7.0.1 automaticky primární instalací. Když je nainstalována IBM WebSphere MQ verze 7.0.1, nemůžete změnit, která instalace je primární instalací. Informace o této volbě a jejích důsledcích naleznete v tématu <a href="#">Více instalací produktu IBM WebSphere MQ, jeden v Version 7.0.1</a> .
Více instalací: Version 7.1nebo novější.	Version 7.1nebo novější	Version 7.1nebo novější.	Chcete-li mít více instalací produktu WebSphere MQ ve verzi 7.1 nebo vyšší, můžete zvolit, zda má být jedna z instalací primární. Informace o této volbě najdete v tématu <a href="#">Více instalací produktu IBM WebSphere MQ Version 7.1nebo novější</a> .
	Není	Version 7.1nebo novější.	

### Související pojmy

[Jedna instalace produktu WebSphere MQ verze 7.1nebo novější, nakonfigurovaná jako primární instalace](#)

[Jedna instalace produktu WebSphere MQ verze 7.1nebo novější, nakonfigurovaná jako nepřímá](#)

[Více instalací produktu WebSphere MQ verze 7.1nebo novější](#)

[Více instalací produktu WebSphere MQ, jedna ve verzi 7.0.1](#)

### Související úlohy

[Změna primární instalace](#)

[Výběr umístění instalace](#)

[Plánování instalace](#)

[Výběr názvu instalace](#)

## Samostatná instalace produktu IBM WebSphere MQ Version 7.1nebo novější, konfigurovaná jako primární instalace

Označením IBM WebSphere MQ jako primární přidáte symbolické odkazy nebo globální proměnné prostředí do systému tak, aby příkazy a knihovny produktu IBM WebSphere MQ použité aplikacemi byly automaticky dostupné s minimálním požadovaným nastavením systému.

Rozhodujete, kam se má instalovat produkt IBM WebSphere MQ.

Je-li to možné, nakonfigurujte aplikace a skripty tak, aby používaly cestu vyhledávání systému k vyhledání řídicích příkazů produktu IBM WebSphere MQ nebo knihoven IBM WebSphere MQ . Tato konfigurace aplikací a skriptů poskytuje maximální flexibilitu pro plnění budoucích úloh, jako je migrace na další vydání produktu IBM WebSphere MQnebo instalace druhé instalace. Další informace o volbách pro připojení aplikací naleznete v tématu [Připojování aplikací v prostředí s více instalacemi](#).

V systému Windows je první instalace automaticky konfigurována jako primární instalace. Na platformách UNIX and Linux musí být první instalace do systému ručně nakonfigurována tak, aby byla primární instalací. Nastavte primární instalaci pomocí příkazu **setmqinst** . Další informace najdete v tématu [Odinstalování, upgrade a údržba primární instalace](#).

### Související úlohy

[Změna primární instalace](#)

[Výběr umístění instalace](#)

[Plánování instalace](#)

[Výběr názvu instalace](#)

## Samostatná instalace produktu IBM WebSphere MQ Version 7.1nebo novější, nakonfigurovaná jako neprimární

Pokud instalujete produkt IBM WebSphere MQ Version 7.1nebo novější, jako neprimární, můžete nakonfigurovat cestu ke knihovně pro aplikace k načtení knihoven produktu IBM WebSphere MQ . Na systému Windows jsou některé funkce produktu k dispozici pouze v případě, že je produkt IBM WebSphere MQ konfigurován jako primární.

### Systémy UNIX a Linux

Důsledky spuštění jiné než primární instalace na systému UNIX and Linux jsou:

- Aplikace, které vyhledají své knihovny IBM WebSphere MQ pomocí vestavěné cesty ke knihovně, například RPATH, nemohou tyto knihovny najít, pokud jsou splněny následující podmínky:
  - Produkt IBM WebSphere MQ se instaluje do jiného adresáře z adresáře zadaného v produktu RPATH .
  - V produktu /usr nejsou žádné symbolické odkazy.
- Pokud aplikace vyhledají své knihovny pomocí externí cesty ke knihovně, například LD\_LIBRARY\_PATH, musíte nakonfigurovat cestu k externí knihovně tak, aby obsahovala adresář `MQ_INSTALLATION_PATH/lib` nebo `MQ_INSTALLATION_PATH/lib64` . Příkazy **setmqenv** a **crtmqenv** mohou konfigurovat celou řadu proměnných prostředí v aktuálním shellu, včetně cesty k externí knihovně.
- Většina procesů IBM WebSphere MQ je spuštěna jako setuid/setgid. Výsledkem je, že při načítání uživatelských procedur budou ignorovat cestu k externí knihovně. Uživatelské procedury, které odkazují na knihovny produktu IBM WebSphere MQ , mohou tyto knihovny najít, pouze pokud jsou nalezeny v cestě knihovny vložené v rámci těchto knihoven. Budou vyřešeny v případě, že by v produktu /usr existoval symbolický odkaz. Uživatelské procedury, které mají být spuštěny na produktu IBM WebSphere MQ Version 7.1nebo novější, mohou být nyní sestaveny tak, aby neodkazovaly na knihovny produktu IBM WebSphere MQ vůbec. Místo toho se spoléhají na IBM WebSphere MQ , aby předal funkce na funkci IBM WebSphere MQ , které pak může uživatelská procedura použít. Další informace viz [Psaní a kompilace ukončení a instalovatelných služeb](#) .

Další informace o volbách pro připojení aplikací naleznete v tématu [Připojování aplikací v prostředí s více instalacemi](#).

Na platformách UNIX and Linux není první instalace do systému automaticky konfigurována jako primární instalace. Nicméně jeden symbolický odkaz je obsažen v příkazu `/usr/bin` za účelem vyhledání příkazu **dspmqrver**. Pokud nechcete žádné symbolické odkazy, musíte tento odkaz odebrat pomocí následujícího příkazu:

```
setmqinst -x -p MQ_INSTALLATION_PATH
```

## Systemy Windows

Důsledky spuštění jiné než primární instalace v systému Windows jsou:

- Aplikace běžně vyhledání své knihovny pomocí externí knihovny, PATH. Neexistuje koncept cesty vložené knihovny nebo explicitní umístění knihovny. Je-li instalace neprimární, globální proměnná prostředí PATH neobsahuje instalační adresář produktu IBM WebSphere MQ. V případě aplikací pro vyhledání knihoven IBM WebSphere MQ aktualizujte proměnnou prostředí PATH tak, aby odkazovala na instalační adresář produktu IBM WebSphere MQ. Příkazy **setmqenv** a **crtmqenv** mohou konfigurovat celou řadu proměnných prostředí v aktuálním shellu, včetně cesty k externí knihovně.
- Některé funkce produktu jsou k dispozici pouze v případě, že je instalace konfigurována jako primární instalace; viz [Funkce, které lze použít pouze s primární instalací v systému Windows](#).

Ve výchozím nastavení je v systému Windows první instalace automaticky konfigurována jako primární. Je třeba ručně zrušit výběr jako primární instalaci.

### Související úlohy

[Změna primární instalace](#)

[Výběr umístění instalace](#)

[Plánování instalace](#)

[Výběr názvu instalace](#)

### Související odkazy

[setmqenv](#)

[crtmqenv](#)

## Více instalací produktu IBM WebSphere MQ Version 7.1 nebo novější

Můžete zvolit, zda má být jako primární instalace nakonfigurována jedna z instalací produktu IBM WebSphere MQ Version 7.1 nebo novější. Vaše volba závisí na tom, jak aplikace vyhledají knihovny.

Knihovny produktu IBM WebSphere MQ (například mqm), které jsou dodávány s produktem IBM WebSphere MQ Version 7.1, automaticky používají knihovny úrovně vyžadované správcem front, ke kterému se připojují. To znamená, že za předpokladu, že aplikace umístí své knihovny produktu IBM WebSphere MQ z instalace produktu IBM WebSphere MQ Version 7.1, může se připojit k libovolnému správci front v daném systému. Je-li jedna instalace produktu IBM WebSphere MQ Version 7.1 nakonfigurována jako primární, zajišťuje, že pokud aplikace najde svou knihovnu rozhraní produktu IBM WebSphere MQ, může se aplikace připojit k libovolnému správci front.

Další informace o připojení aplikací v prostředí s více instalačními prostředí naleznete v tématu [Připojení aplikací v prostředí s více instalačními prostředí](#).

Primární instalace se automaticky nezmění, když odinstalujete primární instalaci. Pokud chcete, aby byla primární instalací jiná instalace, musíte ručně nastavit primární instalaci pomocí příkazu **setmqinst**. Další informace najdete v tématu [Odinstalování, upgrade a údržba primární instalace](#).

### Související pojmy

[Více instalací](#)

### Související úlohy

[Změna primární instalace](#)

[Výběr umístění instalace](#)



[Plánování instalace](#)

[Výběr názvu instalace](#)

## Více instalací produktu IBM WebSphere MQ, jeden v Version 7.0.1

IBM WebSphere MQ Version 7.1 nebo pozdější může koexistovat s IBM WebSphere MQ Version 7.0.1 s určitými omezeními.

- V systémech UNIX and Linux lze produkt Version 7.0.1 instalovat pouze v pevném, výchozím umístění, takže v tomto výchozím umístění není možné instalovat produkt Version 7.1 nebo novější.
- Produkt IBM WebSphere MQ Version 7.0.1 je automaticky konfigurován jako primární instalace. V systému UNIX and Linux jsou symbolické odkazy automaticky vytvořeny do příslušných adresářů produktu IBM WebSphere MQ. V systému Windows je vše, co je produkt k dispozici, registrováno globálně. IBM WebSphere MQ Version 7.0.1 musí být instalován tímto způsobem do práce. Takže, kde je nainstalován produkt IBM WebSphere MQ Version 7.0.1, IBM WebSphere MQ Version 7.1 nebo novější, nelze primární instalaci provést.

Knihovny z produktu IBM WebSphere MQ Version 7.1 nebo novější mohou pracovat s libovolným správcem front spuštěnými v rámci produktu IBM WebSphere MQ Version 7.0.1 nebo později. Pokud se aplikace potřebuje připojit ke správcům front spuštěným pod produktem Version 7.0.1 a dále s pozdějšími verzemi, může pokračovat v práci normálně, pokud jsou splněny následující podmínky:

- Přiděluje produkt IBM WebSphere MQ Version 7.1 nebo pozdější knihovny za běhu.
- Používá pouze funkce dostupné v produktu Version 7.0.1.

Další informace o připojení aplikací v prostředí s více instalačními prostředí naleznete v tématu [Připojení aplikací v prostředí s více instalačními prostředí](#).

Když odinstalujete produkt IBM WebSphere MQ Version 7.0.1, primární instalace se automaticky nezmění. Pokud chcete, aby byla primární instalací jiná instalace, musíte ručně nastavit primární instalaci pomocí příkazu **setmqinst**. Další informace najdete v tématu [Odinstalování, upgrade a údržba primární instalace](#).

### Související pojmy

[Více instalací](#)

### Související úlohy

[Výběr umístění instalace](#)

[Plánování instalace](#)

[Výběr názvu instalace](#)

## Plánování vašich požadavků na ukládání a výkon

Musíte nastavit realistické a dosažitelné úložiště a výkonnostní cíle pro váš systém IBM WebSphere MQ. Použijte odkazy k vyhledání informací o faktorech, které ovlivňují úložiště a výkon na platformě.

Požadavky se liší v závislosti na systémech, na kterých používáte produkt IBM WebSphere MQ, a které komponenty chcete použít.

Nejnovější informace o podporovaných hardwarových a softwarových prostředích naleznete na webové stránce [Systémové požadavky pro produkt IBM WebSphere MQ](#) :

[www.ibm.com/software/integration/wmq/requirements/](http://www.ibm.com/software/integration/wmq/requirements/)

Produkt IBM WebSphere MQ ukládá data správce front do systému souborů. Použijte následující odkazy, abyste zjistili informace o plánování a konfiguraci adresářových struktur pro použití s produktem IBM WebSphere MQ:

- [“Plánování podpory systému souborů” na stránce 122](#)
- [“Požadavky na sdílené systémy souborů” na stránce 123](#)
- [“Sdílení souborů IBM WebSphere MQ” na stránce 132](#)



- [“Adresářová struktura v systémech UNIX and Linux” na stránce 135](#)
- [“Adresářová struktura v systémech Windows” na stránce 144](#)

Pomocí následujících odkazů získáte informace o systémových prostředcích, sdílené paměti a priority procesu na systému UNIX and Linux:

- [“Zdroje pro produkt IBM WebSphere MQ a UNIX System V IPC” na stránce 147](#)
- [“Sdílená paměť v systému AIX” na stránce 148](#)
- [“Priorita procesu WebSphere MQ a UNIX” na stránce 148](#)

### Související pojmy

[“Naplánování” na stránce 5](#)

Při plánování vašeho prostředí IBM WebSphere MQ musíte vzít v úvahu architekturu IBM WebSphere MQ, kterou chcete konfigurovat, požadavky na prostředky, potřebu protokolování a zálohování. Pomocí odkazů v tomto tématu můžete naplánovat prostředí, v němž je produkt IBM WebSphere MQ spuštěn.

[“Návrh architektury produktu IBM WebSphere MQ” na stránce 14](#)

Zjistěte si informace o různých architekturách, které produkt IBM WebSphere MQ podporuje pro styly systému zpráv typu point-to-point a publikování/odběr.

[Hardwarové a softwarové požadavky na systémech UNIX a Linux](#)

[Hardwarové a softwarové požadavky na systému Windows](#)

## Požadavky na prostor na disku

Požadavky na úložný prostor produktu WebSphere MQ závisí na tom, které komponenty instalujete a kolik pracovního prostoru budete potřebovat.

Diskové úložiště se požaduje pro volitelné komponenty, které se rozhodnete instalovat, včetně všech požadovaných komponent, které vyžadují. Požadavek na celkové úložiště závisí také na počtu používaných front, počtu a velikosti zpráv ve frontách a na tom, zda jsou zprávy trvalé. Požadujete také archivační kapacity na disku, pásce nebo jiném médiu, stejně jako prostor pro vaše vlastní aplikační programy.

Následující tabulka zobrazuje přibližný prostor na disku, který se požaduje při instalaci různých kombinací produktu na různých platformách. (Hodnoty se zaokrouhlují nahoru na nejbližší 5 MB, kde je MB 1 048 576 bajtů.)

Platforma	Instalace klienta <sup>1</sup>	Instalace serveru <sup>2</sup>	Instalace produktu WebSphere MQ MFT <sup>3</sup>	Úplná instalace <sup>4</sup>
AIX	145 MB	190 MB	705 MB	915 MB
HP-UX	225 MB	310 MB	1075 MB	1340 MB
IBM i	215 MB	450 MB	80 MB	655 MB
Linux pro System x (32 bitů)	85 MB	N/A	N/A	120 MB
Linux pro System x (64 bitů)	125 MB	170 MB	575 MB	935 MB
Linux v systémech POWER-Big Endian	130 MB	170 MB	565 MB	715 MB
Solaris x86-64, AMD64, EM64Ta kompatibilní procesory	105 MB <sup>5</sup>	150 MB <sup>5</sup>	695 MB	860 MB
Solaris SPARC	105 MB <sup>5</sup>	150 MB <sup>5</sup>	680 MB	820 MB

Platforma	Instalace klienta <sup>1</sup>	Instalace serveru <sup>2</sup>	Instalace produktu WebSphere MQ MFT <sup>3</sup>	Úplná instalace <sup>4</sup>
Windows (32bitová instalace) <sup>6</sup>	390 MB	N/A	N/A	475 MB
Windows (64bitová instalace) <sup>6</sup>	445 MB	555 MB	710 MB	1005 MB

## Poznámky k použití

1. Instalace klienta zahrnuje následující komponenty:

- Běžové prostředí
- Klient


2. Instalace serveru zahrnuje následující komponenty:


- Běžové prostředí
- Server

3. Instalace produktu IBM WebSphere MQ Managed File Transfer zahrnuje následující komponenty:

- IBM WebSphere MQ Managed File Transfer Služba, zapisovače protokolu, agent, nástroje a základní komponenty
- Běžové prostředí
- Server
- Java
- JRE

4. Úplná instalace zahrnuje všechny dostupné komponenty.

5.  Na platformách Solaris je třeba provést bezobslužnou instalaci pro získání této kombinace komponent.

6.  Ne všechny zde uvedené komponenty jsou instalovatelné funkce v systémech Windows ; jejich funkčnost je někdy zahrnuta do jiných funkcí. Viz téma [Funkce produktu WebSphere MQ pro systémy Windows](#).

## Související úlohy

[Výběr, co se má instalovat](#)

## Plánování podpory systému souborů

Data správce front jsou uložena v systému souborů. Správce front využívá zamykání systému souborů k zabránění, aby více instancí správce front s více instancemi bylo současně aktivních.

### Sdílené systémy souborů

Sdílené systémy souborů umožňují současně přistupovat k jednomu fyzickému úložnému zařízení více systémů. K poškození může dojít v případě, že více systémů přistupuje ke stejnému fyzickému úložnému zařízení přímo, aniž by došlo k vynucnutí blokování a řízení souběžnosti. Operační systémy poskytují lokální systémy souborů s uzamčením a řízením souběžnosti pro lokální procesy; síťové systémy souborů poskytují zamykání a řízení souběžnosti pro distribuované systémy.

Historicky nebyly síťové systémy souborů prováděny dostatečně rychle nebo poskytly dostatečné uzamčení a řízení souběžnosti, aby splňovaly požadavky na protokolování zpráv. Dnes mohou síťové systémy souborů zajistit dobrou výkonnost a implementace spolehlivých protokolů síťového systému souborů, jako například *RFC 3530, Network File System (NFS) verze 4 protocol*, splňují požadavky na spolehlivé protokolování zpráv.

## Sdílené systémy souborů a WebSphere MQ

Data správce front pro správce front s více instancemi jsou uložena ve sdíleném síťovém systému souborů. V systémech Microsoft Windows, UNIX and Linux , musí být datové soubory správce front a soubory protokolů umístěny ve sdíleném síťovém systému souborů.

Před verzí produktu v7.0.1produkt WebSphere MQ nepodporuje data správce front uložená v úložišti síťového serveru, k němuž se přistupuje jako ke sdílenému systému souborů. Jsou-li data správce front umístěna ve sdíleném síťovém úložišti, je třeba zajistit, aby k datům správce front nebyla v daném okamžiku spuštěna jiná instance správce front.

Počínaje verzí v7.0.1 používá produkt WebSphere MQ zámek, aby zabránil více instancím stejného správce front s více instancemi současně. Stejně zamykání také zajišťuje, že dva oddělené správce front nemohou nechtěně používat stejnou sadu datových souborů správce front. Pouze jedna instance správce front může mít svůj zámek v daném okamžiku. V důsledku toho produkt WebSphere MQ podporuje data správce front uložená v rámci síťového úložiště, ke kterému se přistupuje jako ke sdílenému systému souborů.

Protože ne všechny blokovací protokoly síťových systémů souborů jsou robustní, a protože systém souborů může být nakonfigurován pro výkon spíše než integritu dat, musíte spustit příkaz **amqmfsc** , který otestuje, zda síťový systém souborů bude řídit přístup k datům a žurnály správce front správně. Tento příkaz používá pouze systémy UNIX a IBM i. V systému Microsoft Windowsnení k dispozici pouze jeden podporovaný síťový systém souborů a příkaz **amqmfsc** není povinný.

### Související úlohy

[“Ověření chování sdíleného systému souborů” na stránce 125](#)

Spusťte **amqmfsc** a zkontrolujte, zda sdílený systém souborů v systémech UNIX splňuje požadavky pro uložení dat správce front pro správce front s více instancemi. Chcete-li demonstrovat, že správce front udržuje integritu zpráv během selhání, spusťte ukázkový program IBM WebSphere MQ MQI client **amqsfhac** paralelně s produktem **amqmfsc** .

## Požadavky na sdílené systémy souborů

Sdílené systémy souborů musí poskytovat integritu zápisu dat, zaručenému výlučnému přístupu k souborům a uvolnění zámeků při selhání práce s produktem IBM WebSphere MQ.

### Požadavky, které musí sdílet sdílený systém souborů

Existují tři základní požadavky, které musí sdílený systém souborů splňovat, aby spolehlivě protokolované zprávy:

#### 1. Integrita zápisu dat

Integrita zápisu dat se někdy nazývá *Write through to disk on flush*. Správce front musí být schopen provést synchronizaci s daty, která jsou úspěšně potvrzena na fyzickém zařízení. V transakčním systému je třeba se ujistit, že některé zápisy byly bezpečně potvrzeny, než budete pokračovat v dalším zpracování.

Konkrétněji, IBM WebSphere MQ na platformách UNIX používá otevřenou volbu `O_SYNC` a systémové volání `fsync()` pro explicitní vynucení zápisu na obnovitelné médium a je závislé na těchto volbách fungují správně.



**Upozornění:** Linux Měli byste připojit systém souborů s volbou `async` , která stále podporuje volbu synchronních zápisů, a poskytuje lepší výkon než volba `sync` .

Všimněte si však, že pokud byl systém souborů exportován z produktu Linux, musíte stále exportovat systém souborů pomocí volby `sync` .

#### 2. Zaručený výhradní přístup k souborům

Chcete-li synchronizovat více správců front, je třeba vytvořit pro správce front mechanismus, který získá výlučný zámek na soubor.

### 3. Uvolnit zámky při selhání

Pokud správce front selže nebo pokud dojde k selhání komunikace se systémem souborů, soubory zamčené správcem front je třeba odemknout a zpřístupnit ostatním procesům, aniž by bylo třeba znovu čekat na opětovné připojení správce front k systému souborů.

Sdílený systém souborů musí splňovat tyto požadavky, aby produkt IBM WebSphere MQ fungoval spolehlivě. Pokud tomu tak není, dojde k poškození dat a protokolů správce front při použití sdíleného systému souborů v konfiguraci správce front s více instancemi.

U správců front s více instancemi na systému Microsoft Windows musí být k síťovému úložišti přistupovat prostřednictvím protokolu CIFS (Common Internet File System) používaného sítěmi Microsoft Windows. Klient CIFS (Common Internet File System) nesplňuje požadavky produktu IBM WebSphere MQ pro sémantiku zamykání na jiných platformách než Microsoft Windows, takže správci front s více instancemi, kteří jsou spuštěni na platformách jiných než Microsoft Windows, nesmí používat CIFS (Common Internet File System) jako svůj sdílený systém souborů.

Pro správce front s více instancemi na jiných podporovaných platformách musí být k úložišti přistupovat prostřednictvím protokolu síťového systému souborů, který vyhovuje Posix, a podporuje zamykání na základě pronájmu. Moderní systémy souborů, jako je síťový systém souborů (NFS) verze 4, používají pronajaté zámky k detekci selhání a poté uvolní zámky po selhání. Starší systémy souborů, jako je například síťový systém souborů verze 3, které nemají spolehlivý mechanismus k uvolnění zámek po selhání, nesmí být použity pro správce front s více instancemi.

### Kontroluje, zda sdílený systém souborů splňuje požadavky

Musíte zkontrolovat, zda sdílený systém souborů, který plánujete použít, splňuje tyto požadavky. Musíte také zkontrolovat, zda je systém souborů správně konfigurován pro spolehlivost. Sdílené systémy souborů někdy poskytují konfigurační volby pro zlepšení výkonu na úkor spolehlivosti.

Za normálních okolností IBM WebSphere MQ pracuje správně s ukládáním atributů do mezipaměti a není nutné vypnout ukládání do mezipaměti, například nastavením NOAC na připojení NFS. Ukládání do mezipaměti pro atributy může způsobit problémy, když více klientů systému souborů soupeří o přístup pro zápis ke stejnému souboru na serveru systému souborů, protože atributy uložené v mezipaměti použité každým klientem nemusí být stejné jako ty atributy na serveru. Příklad souborů, k nimž se přistupuje tímto způsobem, jsou protokoly chyb správce front pro správce front s více instancemi. Protokoly chyb správce front mohou být zapsány jak aktivní, tak i záložní instance správce front a atributy souboru uložené v mezipaměti mohou způsobit nárůst počtu protokolů chyb, než se očekávalo, než se provede rolování souborů.

Chcete-li pomoci se podívat na systém souborů, spusťte úlohu "[Ověření chování sdíleného systému souborů](#)" na stránce 125. Tato úloha kontroluje, zda váš sdílený systém souborů splňuje požadavky 2 a 3. Musíte ověřit požadavek 1 v dokumentaci ke sdílenému systému souborů nebo experimentováním s protokolováním dat na disk.

Selhání disku může způsobit chyby při zápisu na disk, který IBM WebSphere MQ hlásí chyby FFDC (First Failure Data Capture). Můžete spustit kontrolora systému souborů pro váš operační systém, abyste zkontrolovali sdílený systém souborů pro všechny chyby disku. Například na platformách UNIX a Linux se kontrola systému souborů nazývá fsck. Na platformách Windows se kontrola systému souborů nazývá CHKDSK nebo SCANDISK.

### Zabezpečení serveru NFS

**Poznámka:** Měli byste umístit pouze data správce front na server NFS (Network File System). Na systému NFS použijte k zajištění zabezpečení systému následující tři volby s příkazem mount:

#### **noexec**

Pomocí této volby zabráníte spuštění binárních souborů na systému NFS, což zabrání vzdálenému uživateli v spuštění nežádoucího kódu v systému.

## nosuid

Pomocí této volby zabráníte použití bitů set-user-identifier a set-group-identifier, což zabrání vzdálenému uživateli získat vyšší oprávnění.

## nodev

Pomocí této volby zastavíte používání nebo definování speciálních zařízení nebo blokových speciálních zařízení, která zabrání vzdálenému uživateli dostat se z vězení chroot.

## Ověření chování sdíleného systému souborů

Spusťte **amqmfsc** a zkontrolujte, zda sdílený systém souborů v systémech UNIX splňuje požadavky pro uložení dat správce front pro správce front s více instancemi. Chcete-li demonstrovat, že správce front udržuje integritu zpráv během selhání, spusťte ukázkový program IBM WebSphere MQ MQI client **amqsfhac** paralelně s produktem **amqmfsc**.

## Než začnete

Potřebujete server se síťovým úložištěm a dva další servery připojené k serveru, které mají instalovaný produkt WebSphere MQ. Chcete-li konfigurovat systém souborů, musíte mít oprávnění administrátora (root) a být administrátorem produktu WebSphere MQ, aby spustil produkt **amqmfsc**.

## Informace o této úloze

“Požadavky na sdílené systémy souborů” na stránce 123 popisuje požadavky na systém souborů pro použití sdíleného systému souborů s více správci front pro více instancí. Technická poznámka IBM WebSphere MQ [Testování a podpora příkazů pro správce front pro více instancí produktu WebSphere MQ](#) uvádí seznam sdílených systémů souborů, se kterými již produkt IBM testoval. Postup v této úloze popisuje, jak testovat systém souborů, který vám pomůže posoudit, zda neuvedený systém souborů zachovává integritu dat.

Překonání selhání správce front s více instancemi může být spuštěno selháním hardwaru nebo softwaru, včetně problémů s připojením do sítě, které správci front brání zápisu do svých dat nebo souborů protokolu. Hlavně, že máte zájem způsobit selhání na souborovém serveru. Ale musíte také způsobit selhání serverů IBM WebSphere MQ, abyste otestují všechny zámky, které jsou úspěšně uvolněny. Chcete-li důvěřovat ve sdíleném systému souborů, otestujte všechna následující selhání a všechna další selhání, která jsou specifická pro vaše prostředí:

1. Probíhá ukončení běhu operačního systému na souborovém serveru včetně synchronizace disků.
2. Zastavování operačního systému na souborovém serveru bez synchronizace disků.
3. Stiskněte tlačítko reset na každém ze serverů.
4. Vytáčení síťového kabelu z každého ze serverů.
5. Vytáčení napájecího kabelu ze všech serverů.
6. Vypíná každý ze serverů.

Vytvořte adresář v síťovém úložišti, který budete používat ke sdílení dat a protokolů správce front. Vlastníkem adresáře musí být administrátor produktu WebSphere MQ nebo jinými slovy, člen skupiny mqm v systému UNIX. Uživatel, který spouští testy, musí mít oprávnění administrátora WebSphere MQ.

Použijte příklad exportu a připojení systému souborů ve [Vytvořit správce front s více instancemi na systému Linux](#), která vám pomůže při konfiguraci systému souborů. Různé systémy souborů vyžadují různé kroky konfigurace. Přečtěte si dokumentaci k systému souborů.

## Postup

V každé z kontrol zapříčiní všechna selhání v předchozím seznamu, když je spuštěn kontrolor systému souborů. Hodláte-li spustit produkt **amqsfhac** současně s produktem **amqmfsc**, proveďte úlohu “[Spuštění produktu amqsfhac za účelem testování integrity zpráv](#)” na stránce 130 paralelně s touto úlohou.

1. Připojte exportovaný adresář na dva servery IBM WebSphere MQ.

Na serveru systému souborů vytvořte sdílený adresář `shared` a podadresář pro uložení dat pro správce front s více instancemi, `qmda`. Příklad nastavení sdíleného adresáře pro správce front s více instancemi v produktu Linux viz téma Příklad v tématu Vytvoření správce front s více instancemi v produktu Linux.

2. Zkontrolujte základní chování systému souborů.

Na jednom serveru IBM WebSphere MQ spusťte program pro kontrolu systému souborů bez parametrů.

```
amqmfscck /shared/qmda
```

Obrázek 40. Na serveru IBM WebSphere MQ 1

3. Souběžně zapisujete do stejného adresáře z obou serverů IBM WebSphere MQ .

Na obou serverech IBM WebSphere MQ spusťte program pro kontrolu systému souborů současně s volbou `-c` .

```
amqmfscck -c /shared/qmda
```

Obrázek 41. Na serveru IBM WebSphere MQ 1

```
amqmfscck -c /shared/qmda
```

Obrázek 42. Na serveru IBM WebSphere MQ 2

4. Zkontrolujte čekání a uvolnění zámeků na obou serverech IBM WebSphere MQ .

Na obou serverech IBM WebSphere MQ spusťte program pro kontrolu systému souborů současně s volbou `-w` .

```
amqmfscck -w /shared/qmda
```

Obrázek 43. Na serveru IBM WebSphere MQ 1

```
amqmfscck -w /shared/qmda
```

Obrázek 44. Na serveru IBM WebSphere MQ 2

5. Zkontrolujte integritu dat.

a) Naformátujte testovací soubor.

Vytvoření velkého souboru v testovaném adresáři. Soubor je formátován tak, aby následující fáze mohly být úspěšně dokončeny. Soubor musí být dostatečně velký, že je dostatek času na přerušení druhé fáze, aby bylo možné simulovat překonání selhání. Vyzkoušejte výchozí hodnotu 262144 stránek (1 GB). Program automaticky snižuje tuto výchozí hodnotu na pomalých systémech souborů, takže formátování bude dokončeno asi 60 sekund.

```
amqmfscck -f /shared/qmdata
```

Server odpovídá na následující zprávy:

```
Formatting test file for data integrity test.  
Test file formatted with 262144 pages of data.
```

Obrázek 45. Na serveru IBM WebSphere MQ 1

- b) Zapsat data do testovacího souboru pomocí modulu kontroly systému souborů a zároveň způsobit selhání.

Spustíte testovací program na dvou serverech ve stejnou dobu. Spustíte testovací program na serveru, který bude mít zkušenost se selháním, a pak spustíte testovací program na serveru, který bude přežít selhání. Protože selhávání vyšetřujete.

První testovací program se zastaví s chybovou zprávou. Druhý testovací program získá zámek na testovacím souboru a zapíše data do testovacího souboru, od kterého první testovací program zanechal. Nechme druhý testovací program běh k dokončení.

Tabulka 12. Spuštění kontroly integrity dat na dvou serverech ve stejnou dobu	
Server IBM WebSphere MQ 1	Server IBM WebSphere MQ 2
<pre>amqmfscck -a /shared/qmdata</pre>	
<pre>Please start this program on a second machine with the same parameters. File lock acquired. Start a second copy of this program with the same parameters on another server.  Writing data into test file.  To increase the effectiveness of the test, interrupt the writing by ending the process, temporarily breaking the network connection to the networked storage, rebooting the server or turning off the power. To increase the effectiveness of the test, interrupt the writing by ending the process, temporarily breaking the network connection to the networked storage, rebooting the server or turning off the power.</pre>	<pre>amqmfscck -a /shared/qmdata  Waiting for lock... Waiting for lock... Waiting for lock... Waiting for lock... Waiting for lock... Waiting for lock...</pre>
<pre>Turn the power off here</pre>	
	<pre>File lock acquired. Reading test file Checking the integrity of the data read. Appending data into the test file after data already found. The test file is full of data. It is ready to be inspected for data integrity.</pre>

Doba trvání testu závisí na chování systému souborů. Například obvykle trvá 30 až 90 sekund, aby systém souborů uvolnil zámky souboru získané prvním programem po výpadku proudu. Pokud máte příliš málo času na zavedení selhání před vyplněním prvního testovacího programu, použijte volbu -x příkazu **amqmfscck** k odstranění testovacího souboru. Zkuste test od začátku s větším testovacím souborem.

c) Ověřte integritu dat v testovacím souboru.

```
amqmfscck -i /shared/qmdata
```

Server odpovídá na následující zprávy:

```
File lock acquired
Reading test file checking the integrity of the data read.
The data read was consistent.
The tests on the directory completed successfully.
```

*Obrázek 46. Na serveru IBM WebSphere MQ 2*

6. Odstraňte testovací soubory.

```
amqmfscck -x /shared/qmdata
Test files deleted.
```

*Obrázek 47. Na serveru IBM WebSphere MQ 2*

Server odpovídá se zprávou:

```
Test files deleted.
```

## Výsledky

Program vrátí kód ukončení nula, pokud byly testy dokončeny úspěšně, a nenulový jinak.

## Příklady

První sada tří příkladů zobrazuje příkaz produkující minimální výstup.

### Úspěšný test základního zamykání souborů na jednom serveru

```
> amqmfscck /shared/qmdata
The tests on the directory completed successfully.
```

### Selhání testu základního zamykání souborů na jednom serveru

```
> amqmfscck /shared/qmdata
AMQ6245: Error Calling 'write()[2]' on file '/shared/qmdata/amqmfscck.lck' error '2'.
```

### Úspěšný test zamykání na dvou serverech

<i>Tabulka 13. Úspěšné zamykání na dvou serverech</i>	
Server IBM WebSphere MQ 1	Server IBM WebSphere MQ 2
<pre>&gt; amqmfscck -w /shared/qmdata Please start this program on a second machine with the same parameters. Lock acquired. Press Return or terminate the program to release the lock.</pre>	



Tabulka 13. Úspěšné zamykání na dvou serverech (pokračování)

Server IBM WebSphere MQ 1	Server IBM WebSphere MQ 2
	> amqmfscck -w /shared/qmdata Waiting for lock...
[ Return pressed ] Lock released.	
	Lock acquired. The tests on the directory completed successfully

Druhá sada tří příkladů zobrazuje stejné příkazy pomocí režimu s komentářem.

### Úspěšný test základního zamykání souborů na jednom serveru

```
> amqmfscck -v /shared/qmdata
System call: stat("/shared/qmdata")'
System call: fd = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fchmod(fd, 0666)
System call: fstat(fd)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: write(fd)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd1 = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fcntl(fd1, F_SETLK, F_RDLCK)
System call: fd2 = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fcntl(fd2, F_SETLK, F_RDLCK)
System call: close(fd2)
System call: write(fd1)
System call: close(fd1)
The tests on the directory completed successfully.
```

### Selhání testu základního zamykání souborů na jednom serveru

```
> amqmfscck -v /shared/qmdata
System call: stat("/shared/qmdata")
System call: fd = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fchmod(fd, 0666)
System call: fstat(fd)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: write(fd)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_RDLCK)
System call: fdSameFile = open("/shared/qmdata/amqmfscck.lck", O_RDWR, 0666)
System call: fcntl(fdSameFile, F_SETLK, F_RDLCK)
System call: close(fdSameFile)
System call: write(fd)
AMQxxxx: Error calling 'write()[2]' on file '/shared/qmdata/amqmfscck.lck', errno 2
(Permission denied).
```

## Úspěšný test zamykání na dvou serverech

Tabulka 14. Úspěšné uzamčení na dvou serverech-podrobný režim

Server IBM WebSphere MQ 1	Server IBM WebSphere MQ 2
<pre>&gt; amqmfscck -wv /shared/qmdata Calling 'stat("/shared/qmdata")' Calling 'fd = open("/shared/qmdata/ amqmfscck.lkw", O_EXCL   O_CREAT   O_RDWR, 0666)' Calling 'fchmod(fd, 0666)' Calling 'fstat(fd)' Please start this program on a second machine with the same parameters. Calling 'fcntl(fd, F_SETLK, F_WRLCK)' Lock acquired. Press Return or terminate the program to release the lock.</pre>	
	<pre>&gt; amqmfscck -wv /shared/qmdata Calling 'stat("/shared/qmdata")' Calling 'fd = open("/shared/qmdata/ amqmfscck.lkw", O_EXCL   O_CREAT   O_RDWR,0666)' Calling 'fd = open("/shared/qmdata/amqmfscck.lkw, O_RDWR, 0666)' Calling 'fcntl(fd, F_SETLK, F_WRLCK) 'Waiting for lock...</pre>
<pre>[ Return pressed ] Calling 'close(fd)' Lock released.</pre>	
	<pre>Calling 'fcntl(fd, F_SETLK, F_WRLCK)' Lock acquired. The tests on the directory completed successfully</pre>

### Související odkazy

[amqmfscck](#) (kontrola systému souborů)

*Spuštění produktu **amqsfhac** za účelem testování integrity zpráv*

Produkt **amqsfhac** kontroluje, zda správce front používající síťově připojený úložný prostor udržuje integritu dat po selhání.

### Než začnete

Pro tento test jsou zapotřebí čtyři servery. Dva servery pro správce front s více instancemi, jeden pro systém souborů a jeden pro spuštění produktu **amqsfhac** jako aplikace IBM WebSphere MQ MQI client .

Chcete-li nastavit systém souborů pro správce front s více instancemi, postupujte podle kroků [“1”](#) na stránce 125 v části [Procedura](#) .

### Informace o této úloze

#### Postup

1. Vytvořte správce front s více instancemi na jiném serveru QM1 pomocí systému souborů, který jste vytvořili v kroku [“1”](#) na stránce 125 v části [Procedura](#).

Viz téma [Vytvoření správce front s více instancemi](#).

2. Spusťte správce front na obou serverech s vysokou dostupností.

Na serveru 1:

```
strmqm -x QM1
```

Na serveru 2:

```
strmqm -x QM1
```

3. Nastavte připojení klienta ke spuštění produktu **amqsfhac**.

- a) Proceduru v tématu [Ověření instalace klienta](#) použijte k nastavení připojení klienta nebo k příkladným skriptům v části [Ukázky klienta pro opakované připojení](#).
- b) Upravte kanál klienta tak, aby měl dvě adresy IP, odpovídající dvěma serverům, které jsou spuštěny na serveru QM1.

V ukázkovém skriptu upravte:

```
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +  
CONNAME('LOCALHOST(2345)') QMNAME(QM1) REPLACE
```

Do:

```
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +  
CONNAME('server1(2345),server2(2345)') QMNAME(QM1) REPLACE
```

Kde `server1` a `server2` jsou názvy hostitelů těchto dvou serverů a 2345 je port, na kterém naslouchá posluchač kanálu. Obvykle je tato výchozí hodnota nastavena na 1414. Produkt 1414 můžete použít s výchozí konfigurací modulu listener.

4. Vytvořte dvě lokální fronty v produktu QM1 pro test.

Spusťte následující skript MQSC:

```
DEFINE QLOCAL(TARGETQ) REPLACE  
DEFINE QLOCAL(SIDEQ) REPLACE
```

5. Otestujte konfiguraci pomocí produktu **amqsfhac**

```
amqsfhac QM1 TARGETQ SIDEQ 2 2 2
```

6. Integrita testovacích zpráv při testování integrity systému souborů.

Spusťte **amqsfhac** během kroku "5" na stránce 126 procedury [Procedure](#).

```
amqsfhac QM1 TARGETQ SIDEQ 10 20 0
```

Pokud zastavíte aktivní instanci správce front, produkt **amqsfhac** se znovu připojí k jiné instanci správce front, jakmile se stane aktivní. Restartujte zastavenou instanci správce front znovu, abyste mohli selhání vrátit při dalším testu. Pravděpodobně bude třeba zvýšit počet iterací na základě experimentů se svým prostředím tak, aby testovací program byl spuštěn dostatečně dlouho, aby došlo k překonání selhání.

## Výsledky

Příklad spuštění **amqsfhac** v kroku "6" na stránce 131 je zobrazen v [Obrázek 48](#) na stránce 132. Test je úspěšný.

Pokud test zjistil problém, výstup by nahlásil selhání. V některých testech může produkt MQRC\_CALL\_INTERRUPTED vykazovat "Resolving to backed out". Výsledkem je nerozdílný výsledek. Výsledek závisí na tom, zda byl zápis na disk potvrzen v síťovém úložišti souborů před selháním nebo po jeho výskytu.

```
Sample AMQSFHAC start
qmname = QM1
qname = TARGETQ
sidename = SIDEQ
transize = 10
iterations = 20
verbose = 0
Iteration 0
Iteration 1
Iteration 2
Iteration 3
Iteration 4
Iteration 5
Iteration 6
Resolving MQRC_CALL_INTERRUPTED
MQGET browse side tranid=14 pSideinfo->tranid=14
Resolving to committed
Iteration 7
Iteration 8
Iteration 9
Iteration 10
Iteration 11
Iteration 12
Iteration 13
Iteration 14
Iteration 15
Iteration 16
Iteration 17
Iteration 18
Iteration 19
Sample AMQSFHAC end
```

Obrázek 48. Výstup z úspěšného spuštění produktu **amqsfhac**

---

## Související odkazy

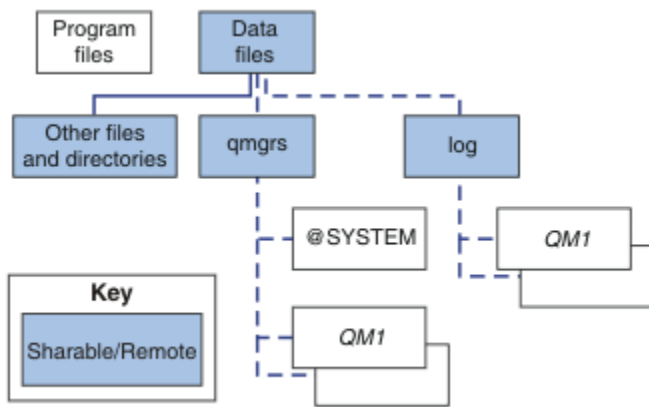
[Ukázkové programy s vysokou dostupností](#)

## Sdílení souborů IBM WebSphere MQ

Některé soubory produktu IBM WebSphere MQ jsou přístupné výhradně aktivním správcem front, jiné soubory jsou sdílené.

Soubory produktu WebSphere MQ jsou rozděleny do programových souborů a datových souborů. Programové soubory jsou obvykle nainstalovány lokálně na každém serveru, kde je spuštěn produkt WebSphere MQ. Správci front sdílejí přístup k datovým souborům a adresářům v rámci výchozího datového adresáře. Požadují výhradní přístup ke svým vlastním adresářovým stromům správce front obsaženým v každém z adresářů `qmgrs` a `log` zobrazených v [Obrázek 49](#) na stránce 133.

Obrázek 49 na stránce 133 je vysokoúrovňový pohled na adresářovou strukturu produktu WebSphere MQ. Zobrazuje adresáře, které lze sdílet mezi správci front a kteří jsou vzdálení. Podrobnosti se liší podle platformy. Tečkovaná čára označuje konfigurovatelné cesty.



Obrázek 49. Celkový pohled na strukturu adresářů produktu WebSphere MQ

### Programové soubory

Adresář souborů programu je obvykle ponechán ve výchozím umístění, je lokální a je sdílen všemi správci front na serveru.

### datové soubory

Adresář datových souborů je obvykle lokální ve výchozím umístění, /var/mqm na systémech UNIX and Linux a konfigurovatelný při instalaci na systému Windows. Je sdíleno mezi správci front. Výchozí umístění můžete nastavit jako vzdálené, ale nesdílet jej mezi různými instalacemi produktu WebSphere MQ. Atribut DefaultPrefix v konfiguraci produktu WebSphere MQ na tuto cestu.

### qmgrs

V produktu v7.0.1 existují dva alternativní způsoby, jak určit umístění dat správce front.

#### Použití Předpona

Atribut Předpona určuje umístění adresáře qmgrs . Produkt WebSphere MQ sestaví název adresáře správce front z názvu správce front a vytvoří jej jako podadresář adresáře qmgrs .

Atribut Předpona je umístěn ve stanze QueueManager a je zděděn od hodnoty v atributu DefaultPrefix . Ve výchozím nastavení správce front pro administrativní zjednodušení obvykle sdílí stejný adresář qmgrs .

Objekt stanza QueueManager je umístěn v souboru mqsc.ini .

Změníte-li umístění adresáře qmgrs pro žádného správce front, je třeba změnit hodnotu atributu Předpona .

Atribut Předpona pro adresář QM1 v produktu [Obrázek 49 na stránce 133](#) pro platformu UNIX and Linux je:

```
Prefix=/var/mqm
```

#### Použití DataPath

Atribut DataPath určuje umístění datového adresáře správce front.

Atribut DataPath uvádí úplnou cestu, včetně názvu datového adresáře správce front. Atribut DataPath se liší od atributu Předpona , který určuje neúplnou cestu k datovému adresáři správce front.

Atribut DataPath , je-li zadán, je umístěn ve stanze QueueManager . Pokud byla zadána, má přednost před každou hodnotou atributu Předpona .

Objekt stanza QueueManager je umístěn v souboru mqsc.ini .

Změníte-li umístění datového adresáře správce front pro libovolného správce front, musíte změnit hodnotu atributu DataPath .

Atribut `DataPath` pro adresář QM1 v produktu [Obrázek 49](#) na stránce 133 pro platformu UNIX nebo Linux je:

```
DataPath=/var/mqm/qmgrs/QM1
```

## log

Adresář protokolů je určen samostatně pro každého správce front v sekci Log v konfiguraci správce front. Konfigurace správce front je v produktu `qm.ini`.

### Podadresáře `DataPath/QmgrName/@IPCC`

Podadresáře `DataPath/QmgrName/@IPCC` se nacházejí v cestě ke sdílenému adresáři. Používají se k vytvoření cesty k adresáři pro objekty systému souborů IPC. Je třeba rozlišovat obor názvů správce front, když je správce front sdílen mezi systémy. Před verzí V7.0.1 byl správce front použit pouze v jednom systému. Jedna sada podadresářů byla dostatečná pro definování cesty k adresáři pro objekty systému souborů IPC, viz [Obrázek 50](#) na stránce 134.

```
DataPath/QmgrName/@IPCC/esem
```

*Obrázek 50. Příklad podadresáře IPC, pre-V7.0.1*

V produktu V7.0.1a vyšší musí být objekty systému souborů IPC rozlišeny systémem. Do cesty k adresáři se přidá podadresář pro každý systém, na kterém je spuštěn správce front, viz [Obrázek 51](#) na stránce 134.

```
DataPath/QmgrName/@IPCC/esem/myHostName/
```

*Obrázek 51. Příklad podadresáře IPC, V7.0.1 a následných vydání*

`myHostName` je až prvních 20 znaků z názvu hostitele vráceného operačním systémem. Na některých systémech může být název hostitele až 64 znaků dlouhý před oseknutím. Vygenerovaná hodnota `myHostName` může způsobit problém ze dvou důvodů:

1. Prvních 20 znaků není jedinečné.
2. Název hostitele je generován algoritmem DHCP, který nealokuje vždy stejný název hostitele do systému.

V těchto případech nastavte `myHostName` pomocí proměnné prostředí `MQC_IPC_HOST`; viz [Obrázek 52](#) na stránce 134.

```
export MQC_IPC_HOST=myHostName
```

*Obrázek 52. Příklad: nastavení MQC\_IPC\_HOST*

### Ostatní soubory a adresáře

Jiné soubory a adresáře, jako je adresář obsahující trasovací soubory a společný protokol chyb, jsou obvykle sdíleny a uchovány v lokálním systému souborů.

Až do verze v7.0.1 se produkt WebSphere MQ spolehl na externí správu a zaručil správcům front výlučný přístup k datům správce front a protokolových souborů. Počínaje verzí v7.0.1 spravuje produkt WebSphere MQ výhradní přístup k těmto souborům pomocí zámků systému souborů. Zámek systému souborů umožňuje aktivní v daném okamžiku pouze jednu instanci určitého správce front.

Když spustíte první instanci konkrétního správce front, převezme vlastnictví svého adresáře správce front. Pokud spustíte druhou instanci, může převzít vlastnictví pouze v případě, že se první instance zastavila. Je-li první správce front stále spuštěn, druhá instance se nespustí a ohlásí, že správce front je spuštěn jinde. Pokud byl zastaven první správce front, převezme vlastnictví správce front i druhý správce front a stane se spuštěným správcem front.

Můžete zautomatizovat proceduru druhého správce front, který přebírá řízení od prvního. Spusťte prvního správce front s volbou `stxmqm -x`, která povoluje jinému správci front převzít jeho obsah. Druhý správce

front pak před pokusem o převzetí vlastnictví souborů správce front vyčká, dokud se soubory správce front nezamknou, a spustí se.

## Adresářová struktura v systémech UNIX and Linux

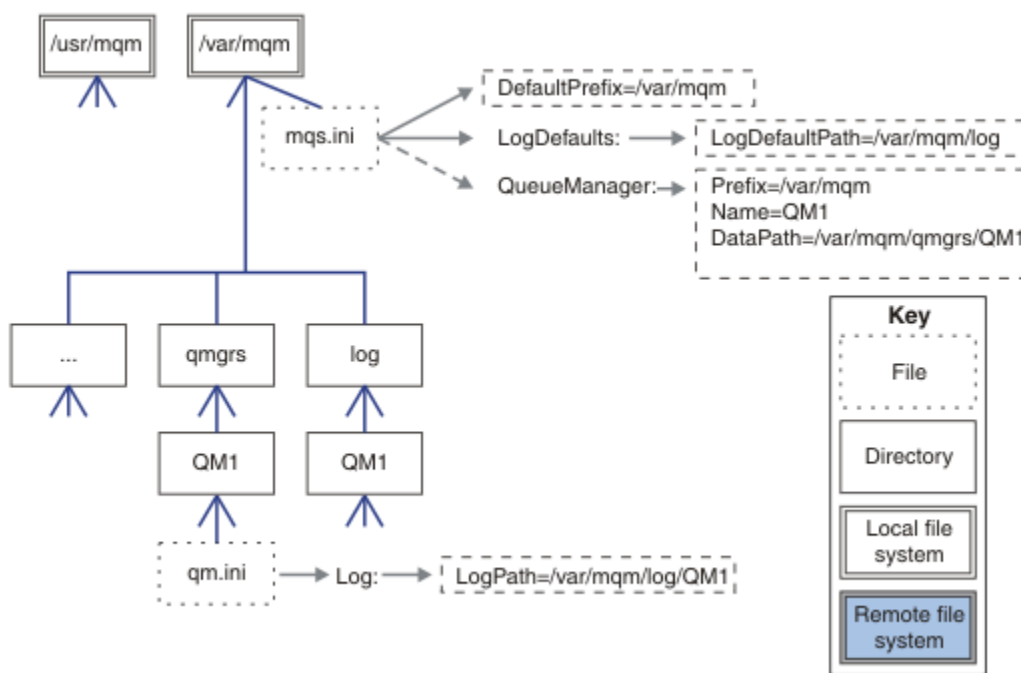
Adresářová struktura produktu WebSphere MQ v systémech UNIX and Linux může být mapována na různé systémy souborů pro snadnější správu, lepší výkon a vyšší spolehlivost.

Využijte flexibilní adresářovou strukturu produktu WebSphere MQ k využití výhod sdílených systémů souborů pro spouštění správců front s více instancemi.

Pomocí příkazu `crtmqm QM1` vytvořte adresářovou strukturu zobrazenou v produktu [Obrázek 53](#) na stránce 135, kde R je vydání produktu. Jedná se o typickou adresářovou strukturu pro správce front vytvořeného v systému WebSphere MQ od verze v7.0.1. Některé adresáře, soubory a nastavení atributu .ini jsou kvůli přehlednosti vynechány a mangování může být změněno jiným názvem správce front. Názvy systémů souborů se liší v různých systémech.

V typické instalaci se každý správce front, kterého vytvoříte, odkazuje na obecné adresáře log a qmgrs v lokálním systému souborů. V konfiguraci s více instancemi jsou adresáře log a qmgrs umístěny v síťovém systému souborů sdíleném s jinou instalací produktu WebSphere MQ.

Obrázek 53 na stránce 135 ukazuje výchozí konfiguraci produktu WebSphere MQ v7.R v systému AIX, kde R je vydání produktu. Příklady alternativních konfigurací s více instancemi najdete v tématu [“Příklad konfigurací adresáře na systémech UNIX and Linux”](#) na stránce 139.



Obrázek 53. Příklad výchozího nastavení WebSphere MQ v7.R adresářová struktura pro systémy UNIX and Linux

Produkt je při výchozím nastavení nainstalován do produktu `/usr/mqm` na systémech AIX a `/opt/mqm` na ostatních systémech. Pracovní adresáře jsou nainstalovány do adresáře `/var/mqm`.

**Poznámka:** Pokud jste vytvořili systém souborů `/var/mqm` před instalací produktu IBM WebSphere MQ, ujistěte se, že má uživatel `mqm` oprávnění k úplnému adresáři, jako je například režim souboru 755.

Adresáře log a qmgrs se zobrazí ve svých výchozích umístěních, jak je definuje výchozí hodnoty atributů `LogDefaultPath` a `DefaultPrefix` v souboru `mqs.ini`. Je-li vytvořen správce front, je při výchozím nastavení vytvořen datový adresář správce front v produktu `DefaultPrefix/qmgrs` a v adresáři `LogDefaultPath /log` se nachází adresář souborů protokolu. `LogDefaultPath` a `DefaultPrefix` mají vliv pouze tehdy, jsou-li správci front a soubory protokolu vytvářeny při výchozím nastavení. Skutečně

umístění adresáře správce front je uloženo v souboru `mq.s.ini` a umístění adresáře souboru protokolu se uloží do souboru `qm.ini`.

Adresář souboru protokolu pro správce front je definován v souboru `qm.ini` v atributu `LogPath`. Použijte volbu `-ld` v příkazu `crtmqm` k nastavení atributu `LogPath` pro správce front, například `crtmqm -ld LogPath QM1`. Vynecháte-li parametr `ld`, použije se místo toho hodnota `LogDefaultPath`.

Datový adresář správce front je definován v atributu `DataPath` ve stanze `QueueManager` v souboru `mq.s.ini`. Volbu `-md` příkazu `crtmqm` použijte k nastavení parametru `DataPath` pro správce front, například `crtmqm -md DataPath QM1`. Pokud vynecháte parametr `md`, bude místo toho použita hodnota atributu `DefaultPrefix` nebo Předpona. Předpona má přednost před `DefaultPrefix`.

Zpravidla vytvořte QM1 specifikující jak protokol protokolů, tak datové adresáře v jednom příkazu.

```
crtmqm  
-md DataPath -ld  
LogPath QM1
```

Můžete upravit umístění protokolu správce front a datových adresářů existujícího správce front úpravou atributů `DataPath` a `LogPath` v souboru `qm.ini`, když je správce front zastaven.

Cesta k adresáři `errors`, stejně jako cesty ke všem ostatním adresářům v produktu `/var/mqm`, není modifikovatelná. Avšak adresáře mohou být připojeny na různých systémech souborů nebo symbolicky propojeny s různými adresáři.

### **Obsah adresáře v systémech UNIX and Linux**

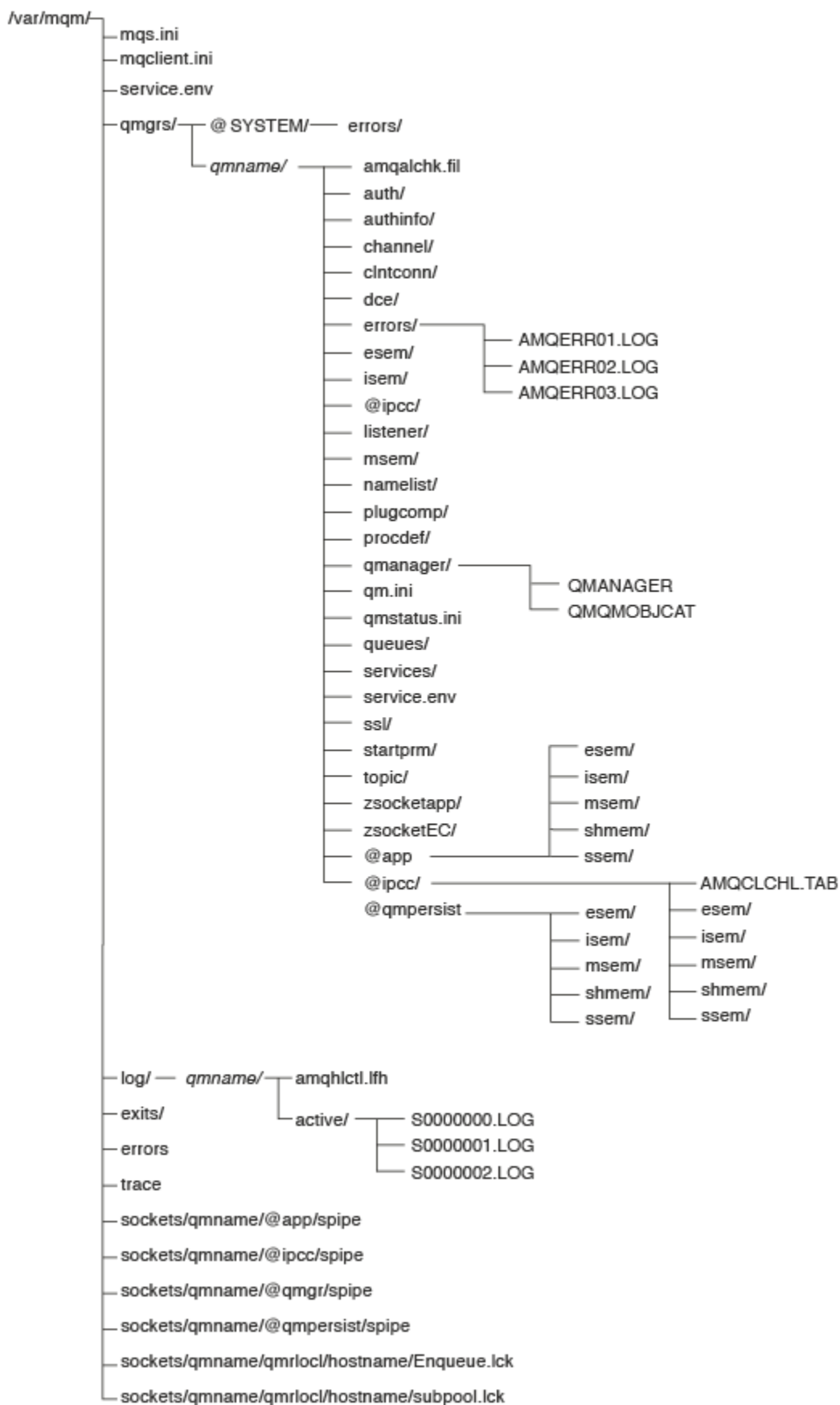
Obsah adresářů přidružených ke správci front.

Informace o umístění souborů produktu naleznete v tématu [Výběr umístění instalace](#).

Další informace o konfiguraci alternativních adresářů najdete v tématu [“Plánování podpory systému souborů”](#) na stránce 122.

V produktu [Obrázek 54](#) na stránce 137 je toto rozvržení reprezentativní pro produkt WebSphere MQ poté, co byl správce front používán již nějakou dobu. Skutečná struktura, která závisí na tom, které operace ve správci front nastaly, se liší.





Obrázek 54. Výchozí adresářová struktura (systémyUNIX) poté, co byl spuštěn správce front

## **/var/mqm/**

Adresář `/var/mqm` obsahuje konfigurační soubory a výstupní adresáře, které se vztahují k instalaci produktu WebSphere MQ jako celku, a nikoli k jednotlivým správcům front.

<b><u>mqs.ini</u></b>	Konfigurační soubor pro celou instalaci produktu WebSphere MQ , přečtěte si, kdy se spustí správce front. Cesta k souboru modifikovatelná pomocí proměnné prostředí <b>AMQ_MQS_INI_LOCATION</b> . Ujistěte se, že je nastavena a exportována v shellu, ve kterém je spuštěn příkaz <b>strmqm</b> .
<b><u>mqclient.ini</u></b>	Výchozí konfigurační soubor klienta načtený klientskými programy WebSphere MQ MQI. Cesta k souboru modifikovatelná pomocí proměnné prostředí <b>MQCLNTCF</b> .
<b><u>service.env</u></b>	Obsahuje proměnné prostředí rozsahu stroje pro proces služby. Cesta k souboru byla opravena.
<b><u>chyby/</u></b>	Protokoly chyb rozsahu stroje a soubory FFST. Cesta k adresáři byla opravena. Viz také FFST: IBM WebSphere MQ pro systémy UNIX and Linux.
<b><u>sokety/</u></b>	Obsahuje informace o každém správci front pouze pro účely systému.
<b><u>trasovat/</u></b>	Trasovací soubory. Cesta k adresáři byla opravena.
<b><u>ukončení/</u></b> <b><u>exits64/</u></b>	Výchozí adresář obsahující uživatelské programy kanálu uživatele. Umístění lze upravit ve stanzách ApiExit v souboru <code>mqs.ini</code> .

## **/var/mqm/qmgrs/qmname/**

`/var/mqm/qmgrs/qmname/` obsahuje adresáře a soubory pro správce front. Tento adresář je uzamknut pro výhradní přístup k aktivní instanci správce front. Cesta k adresáři je přímo modifikovatelná v souboru `mqs.ini` , nebo pomocí volby `md` příkazu `crtmqm` .

<b><u>qm.ini</u></b>	Konfigurační soubor správce front, načten při spuštění správce front.
<b><u>chyby/</u></b>	Protokoly chyb rozsahu správce front. Hodnota <code>qmname</code> = <code>@system</code> obsahuje zprávy související s kanálem pro neznámého nebo nedostupného správce front.
<b><u>@ipcc/</u></b> <b><u>AMQCLCHL.TAB</u></b>	Výchozí řídicí tabulka kanálů klienta, vytvořená serverem WebSphere MQ a načtená klientskými programy WebSphere MQ MQI. Cesta k souboru modifikovatelná pomocí proměnných prostředí <b>MQCHLLIB</b> a <b>MQCHLTAB</b> .
<b><u>QMANAGER</u></b>	Soubor objektů správce front: QMANAGER Katalog objektů správce front: QMQMOBJCAT

Tabulka 16. Dokumentovaný obsah adresáře /var/mqm/qmgrs/qmname na systémech UNIX (pokračování)

<b>authinfo/</b>	Každý objekt definovaný v rámci správce front je přidružen k souboru v těchto adresářích. Název souboru se přibližně shoduje s názvem definice; viz téma <a href="#">Základní informace o názvech souborů produktu WebSphere MQ</a> .
<b>kanál/</b>	
<b>clntconn/</b>	
<b>modul listener/</b>	
<b>seznam názvů/</b>	
<b>procdef/</b>	
<b>fronty/</b>	
<b>služby/</b>	
<b>témata/</b>	
...	Ostatní adresáře používané produktem WebSphere MQ, například @ipcc, mohou být upraveny pouze produktem WebSphere MQ.

### **/var/mqm/log/qmname/**

/var/mqm/log/qmname/ obsahuje soubory protokolu správce front. Tento adresář je uzamknut pro výhradní přístup k aktivní instanci správce front. Cesta k adresáři je modifikovatelná v souboru qm.ini, nebo pomocí volby **ld** příkazu **crtmqm**.

Tabulka 17. Dokumentovaný obsah adresáře /var/mqm/log/qmname na systémech UNIX

<b>amqhlctl.lfh</b>	Řídící soubor protokolu.
<b>aktivní/</b>	Tento adresář obsahuje soubory s protokolem s číslem S0000000.LOG, S0000001.LOG, S0000002.LOGatd.

### **Příklad konfigurací adresáře na systémech UNIX and Linux**

Příklady konfigurace alternativních systémů souborů v systémech UNIX and Linux.

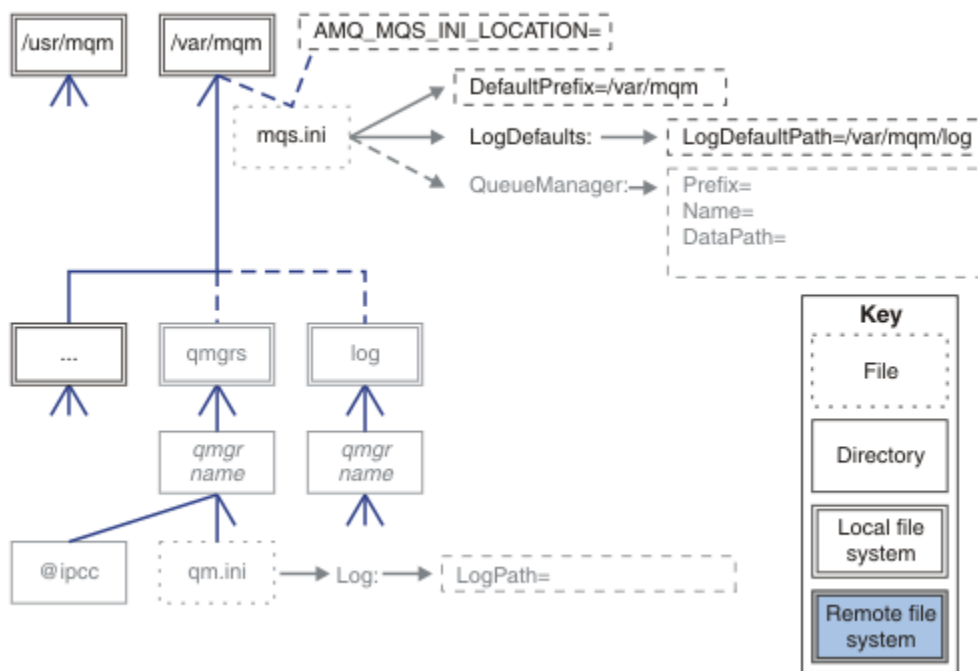
Adresářovou strukturu produktu WebSphere MQ lze přizpůsobit různým způsobem, abyste dosáhli řady různých cílů.

- Chcete-li konfigurovat správce front pro více instancí, umístěte adresáře qmgrs a log na vzdálené sdílené systémy souborů.
- Použijte oddělené systémy souborů pro adresáře dat a protokolů a přiřadte adresáře na různé disky, abyste zlepšili výkon tím, že snížíte soupeření vstupu/výstupu.
- Použijte rychlejší úložná zařízení pro adresáře, které mají větší vliv na výkon. Latence fyzického zařízení je často důležitějším faktorem při výkonu trvalého systému zpráv, než je to, zda je zařízení připojeno lokálně nebo vzdáleně. Následující seznam ukazuje, které adresáře jsou nejvíce a nejméně citlivé na výkon.
  1. log
  2. qmgrs
  3. Ostatní adresáře, včetně /usr/mqm
- Vytvořte adresáře qmgrs a log v systémech souborů, které jsou alokovány pro úložiště s dobrou odolností, jako je například redundantní diskové pole.
- Je lepší ukládat běžné protokoly chyb do var/mqm/errors, lokálně, spíše než na síťový systém souborů, takže chyba související se síťovým systémem souborů může být protokolována.

Obrázek 55 na stránce 140 je šablona, z níž jsou odvozeny jiné adresářové struktury produktu WebSphere MQ. Tečkované čáry v šabloně představují cesty, které lze konfigurovat. V uvedených příkladech

jsou tečkované čáry nahrazeny pevnými řádky, které odpovídají informacím o konfiguraci uloženým v proměnné prostředí AMQ\_MQS\_INI\_LOCATION a v souborech mqs.ini a qm.ini.

**Poznámka:** Informace o cestě se zobrazí tak, jak se objevují v souborech mqs.ini nebo qm.ini. Pokud zadáte parametry cesty v příkazu **crtmqm**, vynechte název adresáře správce front: název správce front bude přidán do cesty produktem WebSphere MQ poté, co došlo k mangování.



Obrázek 55. Šablona vzoru struktury adresáře

Následují příklady konfigurovaných adresářových struktur. První příklad ukazuje typickou výchozí adresářovou strukturu pro produkt WebSphere MQ v7.0.1 vytvořený vyvoláním příkazu **crtmqm QM1**. Druhý příklad ukazuje, jak vypadá typická adresářová struktura pro správce front vytvořeného pomocí verze produktu WebSphere MQ, která je starší než v7.0.1. Adresářová struktura se nezmění.

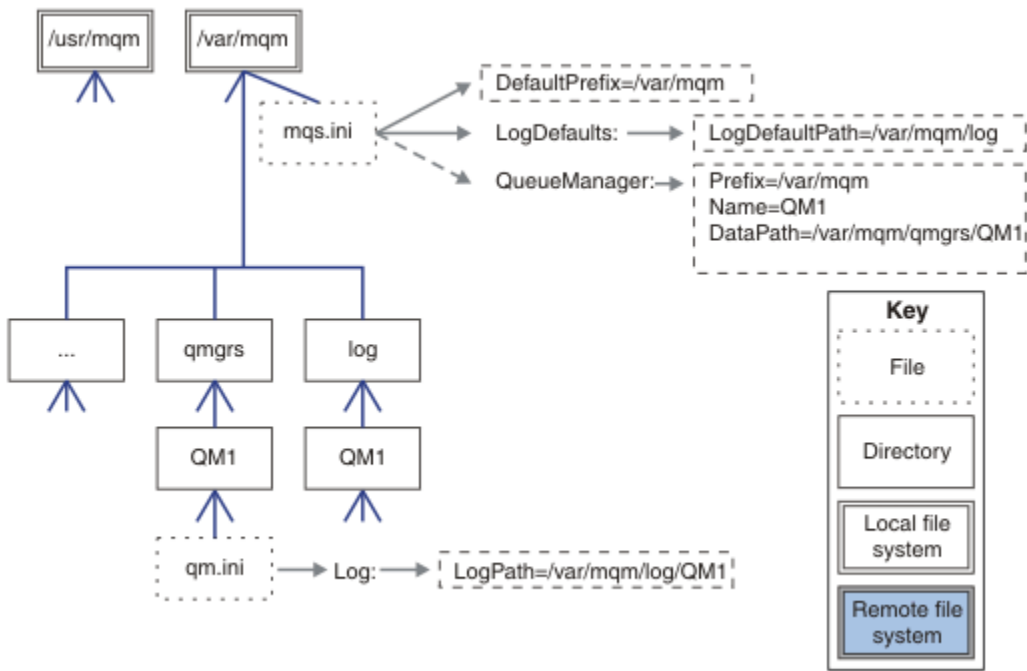
Správci front nově vytvořené ve verzi 7.0.1 mají v dřívějších vydáních produktu v7jiný konfigurační soubor. Pokud potřebujete odebrat opravnou sadu v7.0.1 k opětovnému vrácení na verzi v7.0.0.2, je třeba znovu vytvořit konfigurační soubory. Možná budete muset použít atribut Prefix k definování cesty k novému datovému adresáři správce front nebo byste měli přesunout adresář dat správce front a adresáře protokolu do jiného umístění. Nejbezpečnějším způsobem, jak překonfigurovat správce front, je uložit data a adresáře protokolů správce front, odstranit a znovu vytvořit správce front a poté nahradit data a adresáře protokolů ve svém novém umístění, s těmi, které byly uloženy.

### Typická adresářová struktura pro vydání v7.0.1 dále

Produkt Obrázek 56 na stránce 141 je výchozí adresářová struktura vytvořená v produktu v7.0.1 zadáním příkazu **crtmqm QM1**.

Soubor `mqs.ini` má oddíl pro správce front QM1 vytvořený odkazem na hodnotu `DefaultPrefix`. Objekt stanza `Log` v souboru `qm.ini` má hodnotu pro `LogPath`, který je nastaven odkazem na `LogDefaultPath` v `mqs.ini`.

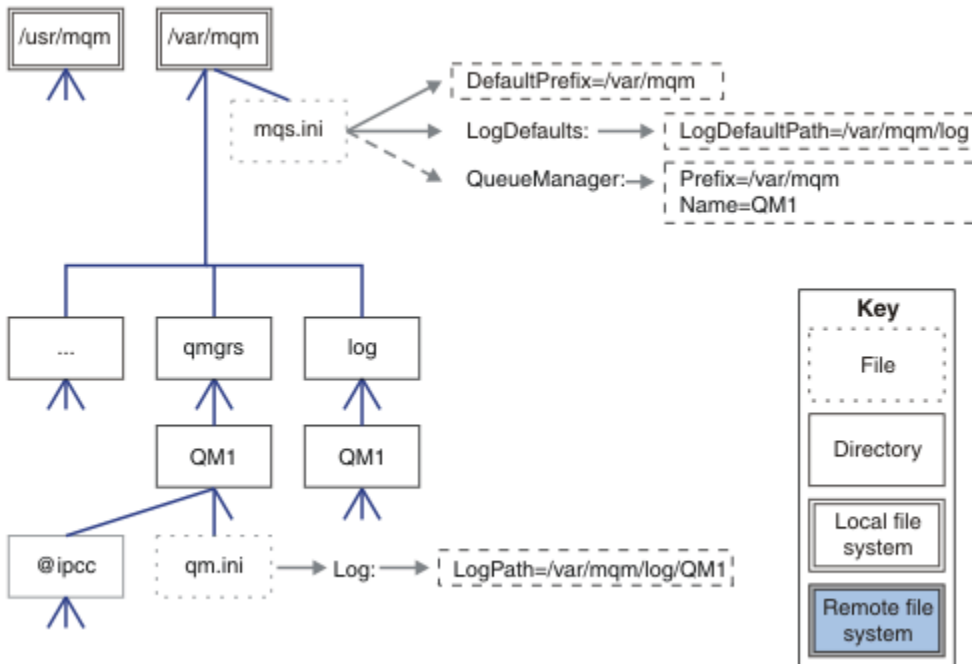
Chcete-li přepsat výchozí hodnoty `DataPath` a `LogPath`, použijte volitelné parametry **crtmqm**.



Obrázek 56. Příklad výchozího nastavení WebSphere MQ v7.R adresářová struktura pro systémy UNIX and Linux

### Typická adresářová struktura pro vydání starší než v7.0.1

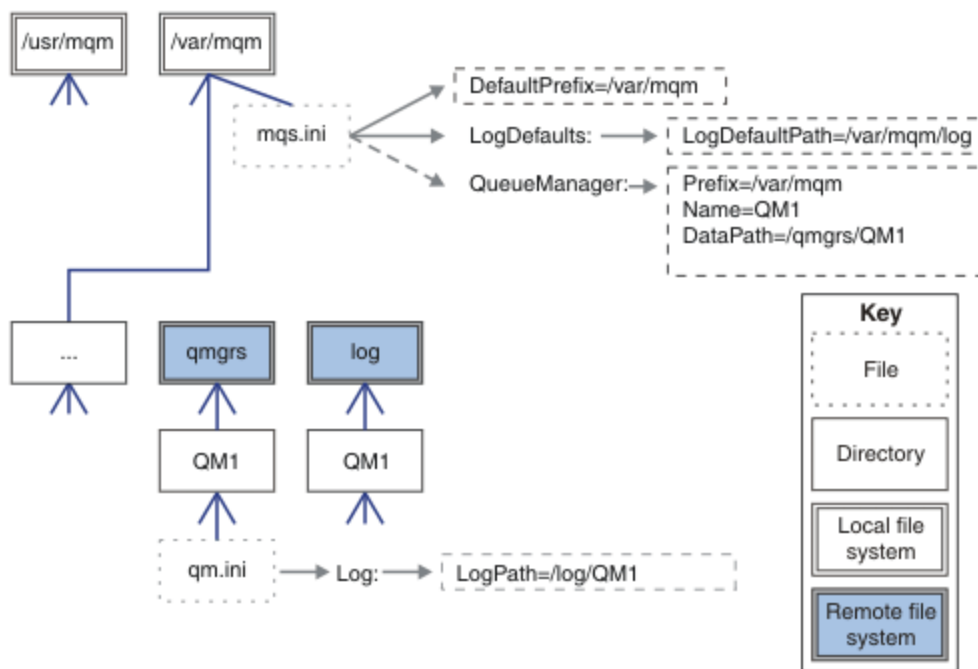
Atribut `DataPath` neexistoval před verzí produktu WebSphere MQ v7.0.1; tento atribut není obsažen v souboru `mqs.ini`. Umístění adresáře `qmgrs` bylo nakonfigurováno pomocí atributu `Předpona`. Umístění jednotlivých adresářů může být konfigurováno pomocí symbolických odkazů, aby ukazovala na různá umístění systému souborů.



Obrázek 57. Typická adresářová struktura pro vydání starší než v7.0.1

## Sdílet výchozí adresáře qmgrs a log (verze v7.0.1 dále)

Alternativou k “Sdílejte vše (vydání v7.0.1 dále)” na stránce 143 je sdílení adresářů qmgrs a log odděleně (Obrázek 58 na stránce 142). V této konfiguraci není třeba nastavit AMQ\_MQS\_INI\_LOCATION jako výchozí soubor mqs.ini, který je uložen v lokálním systému souborů /var/mqm. Soubory a adresáře, jako například mqclient.ini a mqserver.ini, nejsou také sdíleny.

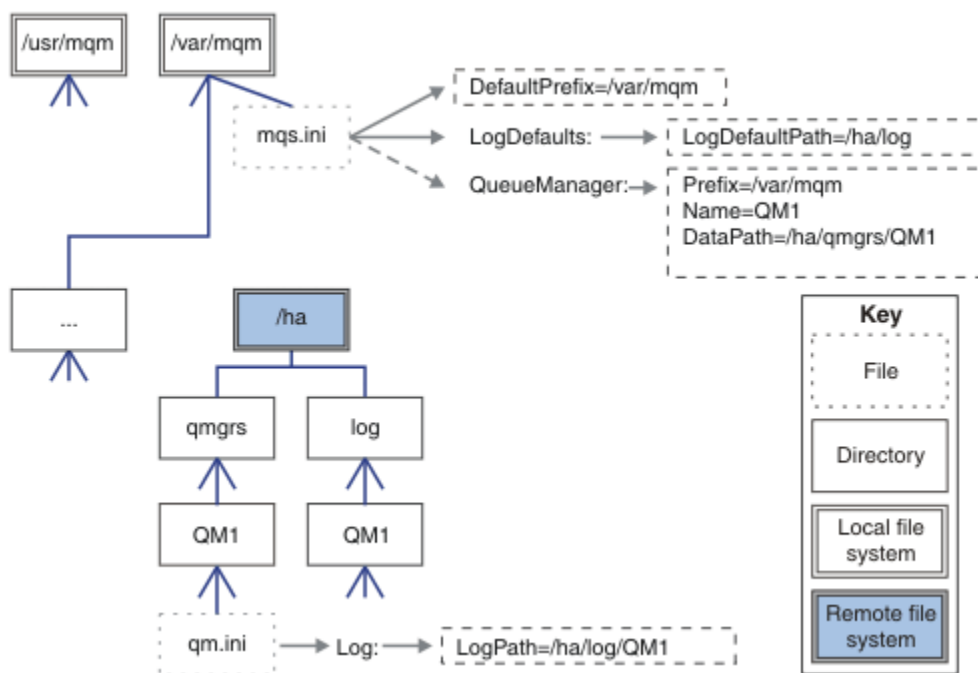


Obrázek 58. Sdílení adresářů qmgrs a log

## Sdílení pojmenovaných adresářů qmgrs a log (verze v7.0.1 dále)

Konfigurace v produktu Obrázek 59 na stránce 143 umístí log a qmgrs do obecného jmenovaného vzdáleného sdíleného systému souborů nazvaného /ha. Stejnou fyzickou konfiguraci lze vytvořit dvěma různými způsoby.

1. Nastavte LogDefaultPath=/ha a pak spusťte příkaz **crtmqm -md /haqmgrs QM1**. Výsledek je přesně tak, jak je ilustrováno v části Obrázek 59 na stránce 143.
2. Ponechejte výchozí cesty nezměněny a pak spusťte příkaz, **crtmqm -ld /ha/log - md /haqmgrs QM1**.



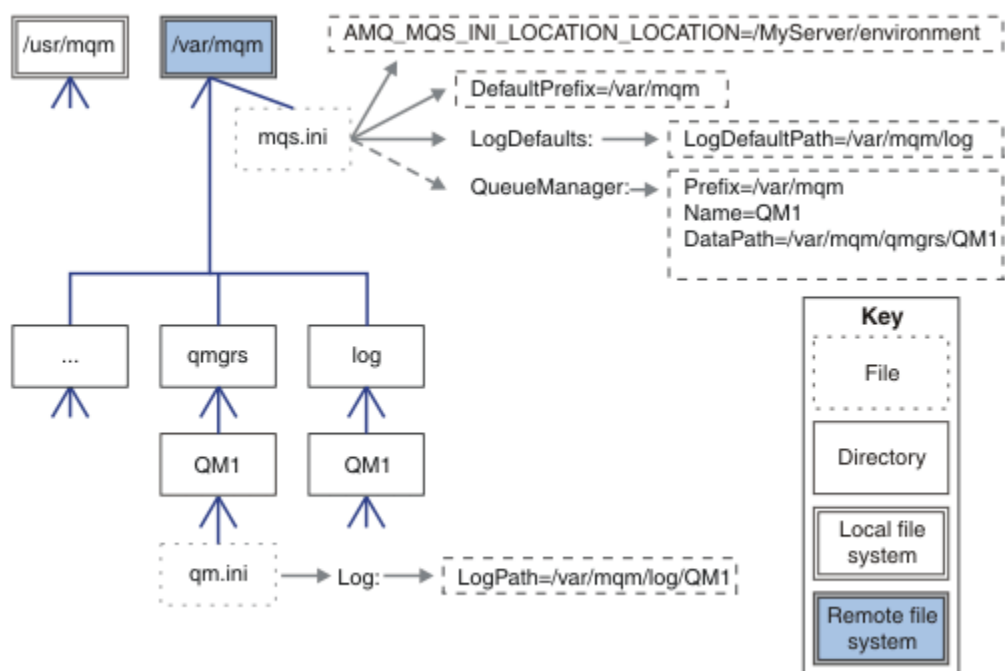
Obrázek 59. Sdílení pojmenovaných adresářů qmgrs a log

### Sdílejte vše (vydání v7.0.1 dále)

Produkt Obrázek 60 na stránce 144 je jednoduchou konfigurací systému s rychlým síťovým úložištěm souborů.

Připojte /var/mqm jako vzdálený sdílený systém souborů. Standardně, když spustíte QM1, vyhledá /var/mqm, najde ho na sdíleném systému souborů a přečte soubor mqs.ini v /var/mqm. Místo použití jednoho souboru /var/mqm/mqs.ini pro správce front na všech serverech můžete nastavit proměnnou prostředí AMQ\_QS\_INI\_LOCATION na každém serveru tak, aby ukazovala na různé soubory mqs.ini.

**Poznámka:** Obsah generického souboru chyb v produktu /var/mqm/errors/ je sdílen mezi správci front na různých serverech.



Obrázek 60. Sdílet vše

Všimněte si, že toto nemůžete použít pro správce front s více instancemi. Důvodem je to, že je nezbytné, aby každý hostitel ve správci front s více instancemi měl vlastní lokální kopii produktu /var/mqm ke sledování lokálních dat, jako jsou například semaforey a sdílená paměť. Tyto entity nemohou být sdíleny mezi hostiteli.

## Adresářová struktura v systémech Windows

Postup vyhledání informací o konfiguraci správce front a adresářů v systému Windows.

Výchozí adresář pro instalaci produktu IBM WebSphere MQ for Windows je:

### 32bitová

C:\Program Files\IBM\WebSphere MQ

### 64 bitů

C:\Program Files (x86)\IBM\WebSphere MQ

Informace o instalaci jsou uloženy v registru Windows. Klíč registru, ve kterém jsou uloženy informace produktu IBM WebSphere MQ:

### 32bitová

My Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\IBM\WebSphere MQ\

### 64 bitů

My Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\IBM\WebSphere MQ\

Každá instalace má specifický dílčí klíč:

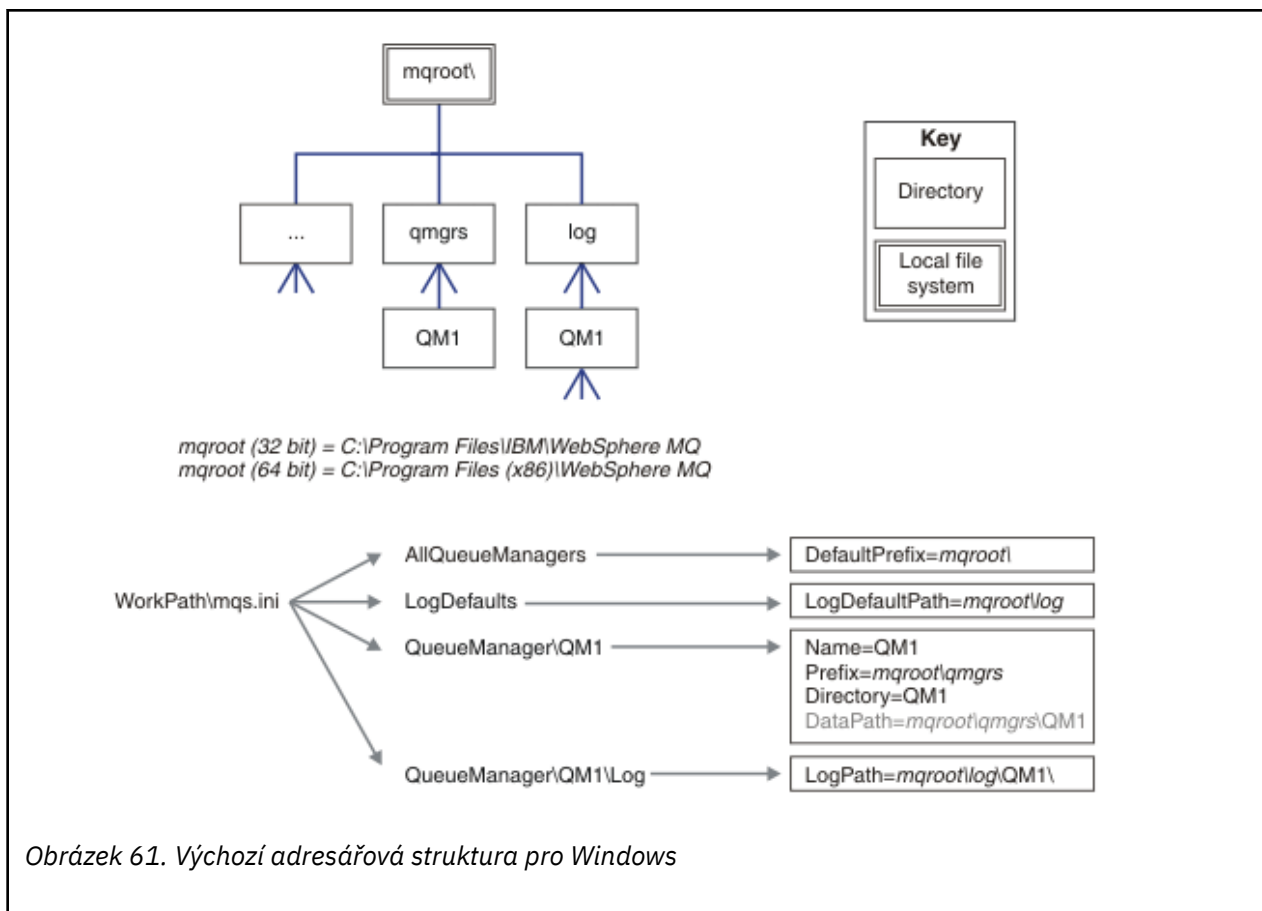
```
Installation\<InstallationName>\
```

Cesta, která ukazuje na datový adresář produktu IBM WebSphere MQ, je uložena do řetězcové hodnoty s názvem *WorkPath* a výchozí adresář pro protokoly je uložen v adresáři *LogDefaultPath*. Datové adresáře správce front jsou vytvářeny v produktu *WorkPath\qmgrs\Qmgrname*. Protokoly správce front jsou vytvářeny v produktu *LogDefaultPath\QmgrName*. Viz [Obrázek 61](#) na stránce 145.

Pokud definujete data správce front a adresáře protokolů při instalaci produktu IBM WebSphere MQ, pak jsou *WorkPath* a *LogDefaultPath* aktualizovány s použitím upravených informací o cestě.

*WorkPath* a *LogDefaultPath* se používají pouze k vytvoření správce front.





## Správci front s více instancemi

Chcete-li nakonfigurovat správce front s více instancemi, musí být datové adresáře protokolu a dat umístěny v síťovém úložišti, pokud možno na jiném serveru, na některý ze serverů, na kterých jsou spuštěny instance správce front.

V příkazu **crtmqm**, **-md** a **-ld** jsou k dispozici dva parametry, aby bylo snazší zadat umístění dat správce front a adresářů protokolů. Efekt zadání parametru **-md** je čtyřnásobně:

1. Stanza `mq5.ini QueueManager\QmgrName` obsahuje novou proměnnou, `DataPath`, která ukazuje na datový adresář správce front. Na rozdíl od proměnné `Předpona` cesta obsahuje název adresáře správce front.
2. Informace o konfiguraci správce front uložené v souboru `mq5.ini` jsou zmenšena na hodnoty `Název`, `Předpona`, `Adresář` a `DataPath`.

## Obsah adresářů

Vypíše umístění a obsah adresářů produktu WebSphere MQ .

Konfigurace produktu WebSphere MQ má tři hlavní sady souborů a adresářů.

1. Spustitelný soubor a další soubory jen pro čtení, jako je soubor README, modul plug-in WebSphere MQ Explorer a soubory nápovědy a soubory licencí, které se aktualizují pouze při použití údržby. Tyto soubory jsou popsány v tématu [Tabulka 18](#) na stránce 146.
2. Potenciálně upravitelné soubory a adresáře, které nejsou specifické pro konkrétního správce front. Tyto soubory a adresáře jsou popsány v tématu [Tabulka 19](#) na stránce 146.
3. Soubory a adresáře, které jsou specifické pro každého správce front na serveru. Tyto soubory a adresáře jsou popsány v tématu [Tabulka 18](#) na stránce 146

## Adresáře a soubory prostředků

Adresáře a soubory prostředků obsahují veškerý spustitelný kód a prostředky pro spuštění správce front. Proměnná *FilePath* klíči registru konfigurace produktu IBM WebSphere MQ specifickou pro instalaci obsahuje cestu k adresářům prostředků.

*Tabulka 18. Adresáře a soubory v adresáři FilePath*

<b>Cesta k souboru</b>	<b>Obsah</b>
<i>FilePath\bin</i>	Příkazy a knihovny DLL
<i>FilePath\bin64</i>	Příkazy a knihovny DLL (64bitové)
<i>FilePath\conv</i>	Tabulky pro převod dat
<i>FilePath\doc</i>	Soubory nápovědy průvodce
<i>FilePath\MQExplorer</i>	Moduly plug-in pro průzkumníka a průzkumníka Eclipse
<i>FilePath\gskit8</i>	Globální sada zabezpečení
<i>FilePath\java</i>	Prostředky Java, včetně JRE
<i>FilePath\licenses</i>	Informace o licenci
<i>FilePath\Non_IBM_License</i>	Informace o licenci
<i>FilePath\properties</i>	Používá se interně
<i>FilePath\Tivoli</i>	
<i>FilePath\tools</i>	Vývojové zdroje a ukázky
<i>FilePath\Uninst</i>	Používá se interně
<i>FilePath\README.TXT</i>	Soubor Readme

## Adresáře, které nejsou specifické pro správce front

Některé adresáře obsahují soubory, jako jsou trasovací soubory a protokoly chyb, které nejsou specifické pro konkrétního správce front. Proměnná *DefaultPrefix* obsahuje cestu k těmto adresářům. Položka *DefaultPrefix* je součástí stanzy *AllQueueManagers*.

*Tabulka 19. Adresáře a soubory v adresáři DefaultPrefix*

<b>Cesta k souboru</b>	<b>Obsah</b>
<i>DefaultPrefix\Config</i>	Používá se interně
<i>DefaultPrefix\conv</i>	Řídicí soubor převodu dat <i>ccsid.tbl</i> popsané v tématu <a href="#">Převod dat</a>
<i>DefaultPrefix\errors</i>	Protokoly chyb nesprávce front, <i>AMQERRnn.LOG</i>
<i>DefaultPrefix\exits</i>	Ukončovací programy kanálu
<i>DefaultPrefix\exits64</i>	Ukončovací programy kanálu (64 bitů)
<i>DefaultPrefix\ipc</i>	Nepoužito
<i>DefaultPrefix\Qmgrs</i>	Popsáno v produktu <a href="#">Tabulka 20 na stránce 147</a>
<i>DefaultPrefix\trace</i>	Trasovací soubory
<i>DefaultPrefix\amqmjpse.txt</i>	Používá se interně

## Adresáře správce front

Při vytváření správce front je vytvořena nová sada adresářů, která je specifická pro správce front.

Pokud vytvoříte správce front s argumentem **-md filepath**, cesta se uloží do proměnné *DataPath* ve stanze správce front v souboru *mq.s.ini*. Pokud vytvoříte správce front bez nastavení parametru **-md filepath**, vytvoří se adresáře správce front v cestě uložené v souboru *DefaultPrefixa* cesta je zkopírována do proměnné *Předpona* ve stanze správce front v souboru *mq.s.ini*.

Tabulka 20. Adresáře a soubory v adresářích <i>DataPath</i> a <i>Prefix/Qmgrs/QmgrName</i>	
Cesta k souboru	Obsah
<i>DataPath</i> \@ipcc	Výchozí umístění pro AMQCLCHL . TAB, tabulka připojení klienta.
<i>DataPath</i> \authinfo	Používá se interně.
<i>DataPath</i> \channel	
<i>DataPath</i> \clntconn	
<i>DataPath</i> \errors	Protokoly chyb, AMQERRnn . LOG
<i>DataPath</i> \listener	Používá se interně.
<i>DataPath</i> \namelist	
<i>DataPath</i> \plugcomp	
<i>DataPath</i> \procdef	
<i>DataPath</i> \qmanager	
<i>DataPath</i> \queues	
<i>DataPath</i> \services	
<i>DataPath</i> \ssl	
<i>DataPath</i> \startpm	
<i>DataPath</i> \topic	
<i>DataPath</i> \active	
<i>DataPath</i> \active.dat	
<i>DataPath</i> \amqalchk.fil	
<i>DataPath</i> \master	
<i>DataPath</i> \master.dat	
<i>DataPath</i> \qm.ini	Konfigurace správce front
<i>DataPath</i> \qmstatus.ini	Stav správce front
<i>Prefix</i> \Qmgrs\QmgrName	Používá se interně
<i>Prefix</i> \Qmgrs\@SYSTEM	Nepoužito
<i>Prefix</i> \Qmgrs\@SYSTEM\errors	

## Zdroje pro produkt IBM WebSphere MQ a UNIX System V IPC

Správce front používá některé prostředky IPC. Použijte **ipcs -a** k vyhledání toho, jaké prostředky se používají.

**Tyto informace platí pouze pro IBM WebSphere MQ spuštěné na systémech UNIX and Linux .**

Produkt IBM WebSphere MQ používá prostředky IPC (System V interprocess communication) (*semafory a segmenty sdílené paměti*) k ukládání a předávání dat mezi komponentami systému. Tyto prostředky jsou používány procesy správce front a aplikacemi, které se připojují ke správci front. Klienti IBM WebSphere MQ MQI nepoužívají prostředky IPC s výjimkou řídicích prvků trasování produktu IBM WebSphere MQ . Použijte příkaz UNIX **ipcs -a** k získání úplných informací o počtu a velikosti prostředků IPC, které se momentálně používají na počítači.

## Sdílená paměť v systému AIX

Pokud se některé typy aplikací nepodaří připojit z důvodu omezení paměti systému AIX , lze ve většině případů tento problém vyřešit nastavením proměnné prostředí EXTSHM=ON.

Některé 32bitové procesy v systému AIX mohou narazit na omezení operačního systému, které má vliv na jejich schopnost připojení ke správčům front WebSphere MQ . Každé standardní připojení k produktu WebSphere MQ používá sdílenou paměť, ale na rozdíl od jiných platforem UNIX and Linux umožňuje AIX 32bitovým procesům připojit pouze 11 sdílené sady paměti.

Většina 32bitových procesů se tento limit nezobrazí, ale aplikace s vysokými požadavky na paměť se nemusí připojit k produktu WebSphere MQ s kódem příčiny 2102: MQRC\_RESOURCE\_PROBLÉM. Tuto chybu mohou zobrazit následující typy aplikací:

- Programy spuštěné ve 32bitových virtuálních počítačích Java
- Programy používající velké nebo velmi velké modely paměti
- Programy, které se připojují k mnoha správčům front nebo databázím
- Programy, které se připojují ke sdíleným paměťovým sadám, na jejich vlastní

Systém AIX nabízí funkci rozšířené sdílené paměti pro 32bitové procesy, která jim umožňuje připojit více sdílené paměti. Chcete-li spustit aplikaci s touto funkcí, exportujte proměnnou prostředí EXTSHM=ON před spuštěním správčů front a vašeho programu. Funkce EXTSHM=ON brání této chybě ve většině případů, ale je nekompatibilní s programy, které používají volbu SHM\_SIZE funkce shmctl.

Toto omezení nemá vliv na klientské aplikace WebSphere MQ MQI a na všechny 64bitové procesy. Mohou se připojit ke správčům front WebSphere MQ bez ohledu na to, zda byla nastavena hodnota EXTSHM.

## Priorita procesů WebSphere MQ a UNIX

Správné postupy při nastavení hodnot priority procesů *nice* .

**Tyto informace platí pro produkt WebSphere MQ spuštěný pouze v systémech UNIX and Linux .**

Spustíte-li proces na pozadí, může být tento proces při vyvolání shellu dán vyšší hodnotou *nice* (a tím nižší prioritou). To může mít obecné důsledky pro výkon produktu WebSphere MQ . V situacích s vysokou prioritou, pokud existuje mnoho připravených podprocesů s vyšší prioritou a některé s nižší prioritou, mohou charakteristiky plánování operačního systému připravit nižší prioritou podprocesů procesorového času.

Je dobrým zvykem, že nezávisle spuštěné procesy přidružené ke správčům front, jako je `runmq1sr`, mají stejné hodnoty *nice* jako správce front, ke kterému jsou přidruženy. Ujistěte se, že shell nepřirazuje těmto procesům na pozadí vyšší hodnotu *nice* . Například v ksh použijte nastavení "`set +o bgnice`" k zastavení ksh ve zvýšení hodnoty *nice* procesů na pozadí. Můžete ověřit hodnoty *nice* spuštěných procesů prozkoumáním sloupce *NI* výpisu "`ps -efl`" .

Také spusťte aplikační procesy produktu WebSphere MQ se stejnou hodnotou *nice* jako správce front. Pokud jsou spuštěny s různými hodnotami *nice* , může podproces aplikace blokovat podproces správce front nebo naopak, který způsobuje snížení výkonu.

# Plánování prostředí klienta IBM WebSphere MQ v systému HP Integrity NonStop Server

Plánujete-li prostředí produktu IBM WebSphere MQ, musíte zvážit prostředí produktu HP Integrity NonStop Server a HP NonStop TMF. Tyto informace použijte k plánování prostředí, ve kterém je spuštěn klient produktu IBM WebSphere MQ pro produkt HP Integrity NonStop Server.

Před plánováním architektury produktu IBM WebSphere MQ pro architekturu HP Integrity NonStop Server se seznamte se základním klientem produktu IBM WebSphere MQ pro koncepty produktu HP Integrity NonStop Server, viz témata v tématu [Klient produktu IBM WebSphere MQ pro technické přehled produktu HP Integrity NonStop Server](#).

## Příprava prostředí produktu HP Integrity NonStop Server

Před instalací musí být prostředí připraveno v závislosti na tom, zda má být instalace ihned ověřena, či nikoli.

Pro instalaci je třeba použít následující položky:

- ID uživatele, které splňuje požadavky. Podrobnosti o požadavcích na ID uživatele naleznete v tématu [Nastavení uživatele a skupiny v systému HP Integrity NonStop Server](#).
- Ověřená umístění v systémech souborů OSS a Guardian, které mohou být určeny pro instalační soubory.
- Operační OSS shell a OSS systém souborů. Systém souborů můžete ověřit provedením následujících úloh:
  - Přihlaste se do prostředí OSS (shell). Ujistěte se, že máte přístup pro zápis do kořenového adresáře instalace OSS, který chcete použít.
  - Přihlaste se do prostředí TACL pomocí ID uživatele ve skupině MQM. Ověřte, že svazek, který chcete použít, splňuje požadavky a je přístupný pro vás a že podsvazek neexistuje.

Můžete se přihlásit k OSS nebo TACL pomocí aliasu, pokud máte jeden nebo váš úplný činitel.

Chcete-li okamžitě pokračovat, abyste ověřili, že je instalace použitelná, budete možná potřebovat také následující volitelné položky:

- Provozní a přístupný lokální subsystém socketů v prostředí OSS.
- Funkční subsystém TCP/IP.

Hodláte-li používat koordinované globální pracovní jednotky TMF, budete potřebovat následující položky:

- Funkční subsystém TMF.
- Operační cesta Pathway (TS/MP).

Obraťte se na administrátora systému, pokud jste v jakékoli pochybnosti o stavu těchto kritických subsystémů.

## IBM WebSphere MQ a HP NonStop TMF

Klient IBM WebSphere MQ for HP Integrity NonStop Server se může podílet na koordinovaných jednotkách práce HP NonStop Transaction Management Facility (HP NonStop TMF). Koordinování transakcí s produktem HP NonStop TMF je podporováno pouze tehdy, je-li správce front v produktu IBM WebSphere MQ Version 7.1 nebo novějším.

Produkt IBM WebSphere MQ poskytuje TMF/Gateway konvertuje transakce z koordinace TMF do koordinace transakcí architektury eXtended Architecture (XA) pro komunikaci se vzdáleným správcem front. Produkt IBM WebSphere MQ poskytuje TMF/Gateway je most mezi transakcemi TMF a správcem front pomocí služeb poskytovaných společností HP NonStop TMF a byl navržen tak, aby běžel v prostředí Pathway.

Software HP NonStop TMF poskytuje ochranu transakcí a konzistenci databáze v náročných prostředích. Další informace o HP NonStop TMF naleznete v příručce [HP NonStop TMF Introduction](#).

Informace o tom, jak nakonfigurovat produkt IBM WebSphere MQ poskytovaný TMF/Gateway, najdete v tématu [Konfigurace produktu HP Integrity NonStop Server](#).

## Použití HP NonStop TMF

Produkt HP NonStop Transaction Management Facility (TMF) je nativní správce transakcí na systému HP Integrity NonStop Server a je integrován se systémem souborů a správci relačních databází, SQL/MP a SQL/MX.

IBM WebSphere MQ klient pro HP Integrity NonStop Server může použít TMF ke koordinaci globálních pracovních jednotek.

Pro koordinaci globálních pracovních jednotek pracuje TMF jako správce transakcí a aplikace musí používat rozhraní API poskytované TMF pro spouštění, potvrzování a odvrácení globálních pracovních jednotek. Aplikace spustí globální pracovní jednotku voláním BEGINTRANSACTION a poté aktualizuje prostředky produktu IBM WebSphere MQ v rámci globální transakce zadáním volání MQPUT, MQPUT1 a MQGET v rámci ovládacího prvku synchronizačního bodu. Aplikace pak může potvrdit globální jednotku práce voláním ENDTRANSACTION, nebo ji vrátit voláním ABORTTRANSACTION.

Aplikace, která používá transakce TMF, může v jednom okamžiku aktivně pracovat pouze na jedné transakci, avšak použití volby RESUMETRANSACTION umožňuje aplikaci přepnout z jedné aktivní transakce do jiné nebo být přidružena k žádné transakci TMF, aniž by bylo nutné dokončit nebo předčasně ukončit dříve aktivní transakci. Jakákoli volání MQPUT, MQPUT1 nebo MQGET se provádí pod aktuálně aktivní transakcí TMF, pokud existuje, nebo lokální transakce, pokud není přítomna. Proto je třeba v rámci žádosti dbát na to, aby tato volání byla prováděna v rámci správné pracovní jednotky.

V rámci globální pracovní jednotky a při aktualizaci prostředků produktu IBM WebSphere MQ může aplikace aktualizovat soubory Enscribe, databáze SQL/MP nebo databáze SQL/MX.

## Použití globálních pracovních jednotek

Globální jednotka práce je implementována jako transakce TMF. Aplikace spustí globální jednotku práce voláním BEGINTRANSACTION a buď potvrdí transakci voláním ENDTRANSACTION, nebo provede odvolání transakce voláním ABORTTRANSACTION. Aplikace může používat i jiná volání rozhraní API TMF.

Aplikace může dědit transakci TMF z jiné aplikace. Například aplikace (první aplikace) může provést práci v rámci transakce před odpovědí a předáním transakce zpět do druhé aplikace za účelem dalšího zpracování. Jak první, tak druhé aplikace se proto mohou účastnit stejné globální pracovní jednotky, která zahrnuje aktualizace front IBM WebSphere MQ a aktualizací souborů a databází. Schopnost předat transakci TMF mezi aplikacemi znamená, že několik aplikací produktu IBM WebSphere MQ může provádět operace systému zpráv v rámci stejné globální transakce.

Aplikace může spravovat a řídit více aktivních transakcí TMF ve stejnou dobu. Transakce může být spuštěna samotnou aplikací nebo zděděnou z jiných aplikací nebo z obou aplikací. To znamená, že se aplikace může podílet na více globálních jednotkách práce současně.

Maximální počet souběžných aktivních transakcí TMF na proces je 1000, což je limit architektury. Pokud aplikace spravuje více transakcí TMF, v každém okamžiku může být aktuální pouze jedna transakce. Jinak žádná z transakcí nemůže být aktuální. Aplikace může používat volání TMF API jako RESUMETRANSACTION, ACTIVATERCEIVETRANSID a TM\_F\_SET\_TX\_ID pro přesun stavu aktuálního stavu z jedné transakce do jiné nebo k určení, že žádná transakce není aktuální. Aplikace používá tuto úroveň řízení k určení, zda je operace systému zpráv prováděna v rámci lokální jednotky práce, globální jednotky práce nebo mimo ovládací prvek synchronizačního bodu:

- Pokud aplikace volá operaci MQPUT, MQPUT1 nebo MQGET v rámci řízení synchronizačního bodu, když není aktuální transakce TMF aktuální, produkt IBM WebSphere MQ zpracuje volání v rámci lokální jednotky práce.
- Pokud aplikace volá operaci MQPUT, MQPUT1 nebo MQGET v rámci synchronizačního bodu, když má aplikace aktuální transakci TMF, produkt IBM WebSphere MQ zpracuje volání v rámci globální jednotky práce, která je implementována aktuální transakcí TMF.

- Pokud aplikace volá operaci MQPUT, MQPUT1 nebo MQGET mimo ovládací prvek synchronizačního bodu, produkt IBM WebSphere MQ zpracuje volání mimo ovládací prvek synchronizačního bodu bez ohledu na to, zda má aplikace aktuální transakci TMF v době volání.

Produkt IBM WebSphere MQ nikdy nemění stav transakce TMF aplikace během volání MQI, s výjimkou případu, kdy dojde k selhání softwaru nebo hardwaru během zpracování a IBM WebSphere MQ nebo operační systém určuje, že transakce musí být vrácena, aby byla zachována integrita dat. Každé volání MQI obnoví stav transakce aplikace těsně před vrácením řízení aplikaci.

## **Vyvarování se přerušitelných transakcí**

Vyhnete se návrhu aplikací, v nichž transakce TMF zůstávají aktivní po dobu delší než několik desítek sekund. Dlouho běžící transakce mohou způsobit, že se cyklický záznam pro audit TMF zaplní. Vzhledem k tomu, že TMF je kritickým systémem celosystémový prostředek, TMF se chrání tím, že zálohuje transakce aplikace, které jsou aktivní příliš dlouho.

Předpokládejme, že zpracování v rámci aplikace je řízeno získáváním zpráv z fronty a že aplikace získá zprávu z fronty a zpracuje zprávu v rámci pracovní jednotky. Obvykle aplikace volá příkaz MQGET s volbou čekání a v rámci ovládacího prvku synchronizačního bodu, aby získal zprávu z fronty.

Pokud aplikace používá místo toho globální pracovní jednotku, musí být zadaný čekací interval na volání MQGET krátký, aby se předešlo dlouhé běžící transakci. To znamená, že aplikace může vyžadovat více než jednou vyvolat volání MQGET, než načte zprávu.





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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#### LICENČNÍ INFORMACE:

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

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

## Informace o programovacím rozhraní

---

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

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

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

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

## Ochranné známky

---

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

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

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

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

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

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







Číslo položky:

(1P) P/N: