9.3

Plánování pro produkt IBM MQ

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 205.

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

Když odešlete informace na adresu IBM, udělujete IBM nevýhradní právo používat nebo distribuovat informace libovolným způsobem, který považuje za odpovídající, aniž by vám tím vznikl jakýkoliv závazek.

Obsah

Naplánování..... 5
IBM MQ typy vydání: aspekty plánování..... 5
IBM MQ a IBM MQ Appliance místní aspekty připravenosti na GDPR..... 8
Architektury založené na jednom správci front..... 17
Architektury založené na více správcích front..... 18
Plánování distribuovaných front a klastrů..... 19
Plánování distribuované sítě publikování/odběru..... 69
Plánování požadavků na úložiště a výkon na platformě Multiplatforms..... 106
Požadavky na místo na disku na platformě Multiplatforms..... 107
Plánování podpory systému souborů na platformě Multiplatforms..... 111
Plánování podpory systému souborů pro produkt MFT na platformě Multiplatforms..... 138
Volba kruhového nebo lineárního protokolování na platformě Multiplatforms..... 139
Sdílená paměť v systému AIX..... 139
Prostředky IBM MQ a UNIX System V IPC..... 140
IBM MQ a UNIX Priorita procesu..... 140
Plánování prostředí IBM MQ na systému z/OS..... 140
Plánování pro vašeho správce front..... 141
Plánování inicializátoru kanálu..... 169
Plánování skupiny sdílení front (QSG)..... 173
Plánování zálohování a obnovy..... 186
Plánování prostředí z/OS UNIX..... 194
Plánování pro Advanced Message Security..... 195
Plánování pro Managed File Transfer..... 196
Plánování použití IBM MQ Console a REST API na z/OS..... 201

Poznámky..... 205
Informace o programovacím rozhraní..... 206
Ochranné známky..... 206

Plánování architektury IBM MQ

Při plánování prostředí IBM MQ zvažte podporu, kterou produkt IBM MQ poskytuje pro jednu a více architektur správců front a pro styly systému zpráv typu point-to-point a publikování/odběr. Také naplánujte své požadavky na prostředky a použití protokolovacích a zálohovacích zařízení.

Informace o této úloze

Před plánováním architektury IBM MQ se seznamte se základními koncepty produktu IBM MQ . Viz IBM MQ Technický přehled.

Architektury systému IBM MQ sahají od jednoduchých architektur používajících jednoho správce front až po složitější sítě vzájemně propojených správců front. Více správců front je propojeno pomocí technik distribuovaného řazení do front. Další informace o plánování architektury jednoho správce front a více správců front naleznete v následujících tématech:

- “Architektury založené na jednom správci front” na stránce 17
- “Architektury založené na více správcích front” na stránce 18
  - “Plánování distribuovaných front a klastrů” na stránce 19
  - “Plánování distribuované sítě publikování/odběru” na stránce 69

z/OS V systému IBM MQ for z/OS můžete používat sdílené fronty a skupiny sdílení front, abyste mohli implementovat vyvažování pracovní zátěže, a vaše aplikace IBM MQ mohou být rozšiřitelné a vysoce dostupné. Informace o sdílených frontách a skupinách sdílení front naleznete v tématu Sdílené fronty a skupiny sdílení front.

Produkt IBM MQ poskytuje dva různé modely vydání:

- Vydání Long Term Support (LTS) je nejvhodnější pro systémy vyžadující dlouhodobou implementaci a maximální stabilitu.
- Vydání Continuous Delivery (CD) je určeno pro systémy, které potřebují rychle využívat nejnovější funkční vylepšení produktu IBM MQ.

Oba typy vydání jsou nainstalovány stejným způsobem, ale existují aspekty týkající se podpory a migrace, které musíte pochopit. Další informace viz IBM MQ typy vydání a správa verzí.

Chcete-li získat informace o plánování více instalací, požadavcích na úložiště a výkon a použití klientů, prohlédněte si další dílčí témata.

Související pojmy

IBM MQ typy vydání a správa verzí

“Plánování prostředí IBM MQ na systému z/OS” na stránce 140
Při plánování prostředí IBM MQ musíte vzít v úvahu požadavky na prostředky pro datové sady, sady stránek, Db2, zařízení Coupling Facilities a prostředky pro protokolování a zálohování. Toto téma použijte k plánování prostředí, kde je spuštěn produkt IBM MQ .

Dostupnost, obnova a restartování

Související úlohy

Kontrola požadavků

Ujistěte se, že zprávy nejsou ztraceny (protokolování)

IBM MQ typy vydání: aspekty plánování

Dva hlavní typy vydání pro IBM MQ jsou Long Term Support (LTS) a Continuous Delivery (CD). Pro každou podporovanou platformu má vámi zvolený typ vydání vliv na řazení, instalaci, údržbu a migraci.

Podrobné informace o typech vydání naleznete v tématu IBM MQ Typy vydání a správa verzí.

Aspekty pro produkt IBM MQ for Multiplatforms

Multi

Řazení

V rámci Passport Advantage existují dvě oddělené eAssemblies pro IBM MQ 9.3. Jeden obsahuje obrazy instalace pro vydání produktu IBM MQ 9.3.0 Long Term Support a druhý obrazy instalace pro vydání produktu IBM MQ 9.3.x Continuous Delivery . Stáhněte obrazy instalace z eAssembly podle vašeho výběru vydání.

Všechny verze produktu IBM MQ a verze produktu IBM MQ 9.3 LTS i CD patří ke stejnému ID produktu.

Oprávnění k užívání produktu IBM MQ se vztahuje na celý produkt (PID) v souladu s omezeními licencovaných komponent a cenových metrik. To znamená, že si můžete svobodně vybrat mezi obrazy instalace produktu LTS release a CD release pro produkt IBM MQ 9.3.

Instalace

Po stažení obrazu instalace z produktu Passport Advantagebyste měli vybrat pro instalaci pouze komponenty, pro které jste zakoupili oprávnění. Další informace o tom, které instalovatelné komponenty jsou zahrnuty pro každou zpoplatněnou komponentu, naleznete v tématu IBM MQ Informace o licenci .

Vydání produktu IBM MQ 9.3.0 LTS a IBM MQ 9.3.x CD můžete nainstalovat na stejný obraz operačního systému. Pokud tak učiníte, komponenty se zobrazí jako samostatné instalace podporované podporou více verzí produktu IBM MQ . Každá verze má různé sady správců front přidružené k této verzi.

Každé nové vydání produktu CD je poskytnuto jako obraz instalace. Nové vydání produktu CD lze instalovat spolu s existujícím vydáním, nebo dřívější vydání produktu CD může instalační program aktualizovat na nové vydání.

Verze produktu CD obsahují funkční vylepšení, stejně jako nejnovější sadu oprav defektů a aktualizací zabezpečení. Každé vydání produktu CD je kumulativní a zcela nahrazuje všechny předchozí verze produktu IBM MQ. Takže můžete přeskočit specifické vydání produktu CD , pokud neobsahuje žádnou funkci, která je relevantní pro váš podnik.

Údržba

Vydání LTS je obsluhováno aplikací opravných sad, které poskytují opravy defektů, a kumulativní aktualizace zabezpečení (CSU), které poskytují opravy zabezpečení. Opravné sady a jednotky CSU jsou pravidelně zpřístupněny a jsou kumulativní.

Pro systém CDjsou jednotky CSU vytvářeny pouze pro nejnovější vydání produktu CD , které může být v následné verzi.

Tým podpory IBM vám může příležitostně nařizovat použití prozatímní opravy. Prozatímní opravy jsou také známé jako nouzové nebo testovací opravy a používají se k použití naléhavých aktualizací, které nemohou čekat na další doručení údržby.

Migrace mezi LTS vydáním a CD vydáním

Existují omezení a omezení, ale obecně lze jednoho správce front migrovat z použití LTS kódu vydání na CD kód vydání, nebo z použití CD kódu vydání na LTS kód vydání, za předpokladu, že cílové vydání je vyšší než vydání používané před migrací.

Jsou možné dva přístupy:

- Nainstalujte nové vydání kódu na místo, aby se aktualizovala existující instalace produktu IBM MQ . Všichni správci front přidružení k instalaci používají při spuštění nové vydání kódu.
- Nainstalujte novou verzi kódu jako novou instalaci a poté přesuňte jednotlivé instance správce front do nové instalace pomocí příkazu setmqm .

Když správce front spustí vydání kódu CD , aktualizuje se úroveň příkazu správce front tak, aby označovala novou úroveň vydání. To znamená, že jsou povoleny všechny nové funkce poskytované ve vydání a že již nelze restartovat správce front s použitím verze kódu s nižším číslem VRM .

Aspekty pro produkt IBM MQ for z/OS

z/OS

Řazení

Při objednávání produktu IBM MQ for z/OS 9.3jsou na webu ShopZk dispozici dvě samostatné funkce. Funkce odpovídají vydání LTS a vydání CD . Obě funkce jsou použitelné pro stejné ID produktu (PID). Jedná se o ID produktu, který je licencován, takže tam, kde je jedna funkce licencována, existuje oprávnění k použití alternativní funkce, je-li to požadováno. Při objednávání vyberte funkci odpovídající buď vydání LTS , nebo vydání CD .

Pokud vybíráte produkty pro zahrnutí do ServerPac, nemůžete vybrat vydání LTS a vydání CD ve stejném pořadí ServerPac , protože produkty nemohou být nainstalovány nástrojem SMP/E ve stejné cílové zóně.

Instalace

Verze LTS a CD jsou poskytovány v samostatných sadách FMID. Všimněte si, že tyto identifikátory FMID nelze nainstalovat do stejné cílové zóny SMP/E. Pokud potřebujete vydání LTS i CD :

- Nainstalujte vydání LTS a CD v oddělených cílových zónách.
- Pro obě vydání udržujte oddělené cílové a distribuční knihovny.

Pokud je správce front ve skupině sdílení front, je při upgradu na nejnovější verzi disku CD nutné provést upgrade všech správců front ve skupině.

Úroveň příkazu správce front je trojciferná úroveň VRM. Program IBM MQ může volat `MQINQ`a předat selektor `MQIA_COMMAND_LEVEL` , aby získal úroveň příkazu správce front, ke kterému je připojen.

Protože vydání používají různá FMID, nemůžete aktualizovat vydání CD s údržbou pro vydání LTS nebo naopak. Podobně neexistuje žádný způsob, jak přepnout verzi kódu produktu z vydání produktu LTS na vydání produktu CD nebo naopak. Můžete však přepínat správce front mezi modely vydání. Viz Migrace mezi vydáním LTS a vydáním CD.

Poznámka:

Verze IBM MQ 9.0.x a IBM MQ 9.1.x CD měly samostatné identifikátory FMID závislé na verzi a vydání. Takže přesun z 9.0.x CD do 9.1.x CD vyžadoval alespoň jednu úplnou instalaci SMP/E.

V produktu IBM MQ for z/OS 9.2.0používá vydání CD sadu FMID, které zůstávají stejné pro všechna vydání produktu IBM MQ for z/OS s číslem verze 9. Vzhledem k tomu, že každá nová verze produktu IBM MQ je k dispozici jako vydání systému CD i LTS , můžete upgradovat vydání produktu CD použitím oprav PTF na jedinou instalaci SMP/E, i když překračujete hranici hlavní verze. Můžete například přejít z IBM MQ for z/OS 9.2.0 CD, na IBM MQ for z/OS 9.2.2 CD, na IBM MQ for z/OS 9.2.4 CD, na IBM MQ for z/OS 9.3.0 CD, pouze pomocí PTF.

Můžete rozlišovat mezi vydáními LTS a CD se stejnou úrovní úpravy uvolnění verze tím, že se podíváte na zprávu CSQY000I v protokolu úlohy správce front.

Údržba

Produkt IBM MQ for z/OS používá opravy PTF pro údržbu.

LTS Opravy PTF jsou specifické pro konkrétní sadu knihoven odpovídající určité úrovni vydání. V případě funkcí UNIX System Services (tj. JMS a WEB UI, Connector Pack a Managed File Transfer) jsou z/OS opravy PTF přímo sladěny s opravnými sadami Multiplatforms a kumulativními aktualizacemi zabezpečení (CSU). Tyto opravy jsou kumulativní a jsou k dispozici současně s ekvivalentní opravnou sadou Multiplatforms nebo CSU.

CD CD CSU nejsou obvykle k dispozici mezi vydáními CD, ale jsou zahrnuty v příštím vydání produktu IBM MQ for z/OS CD . Můžete také kontaktovat podporu a požádat o + + USERMOD.

Ostatní opravy na systému IBM MQ for z/OS jsou odlišné opravy na konkrétních částech. Tyto opravy řeší specifické problémy, nejsou kumulativní a jsou k dispozici v době, kdy jsou vytvářeny.

Migrace mezi LTS vydáním a CD vydáním

Existují omezení a omezení, ale obecně lze jednoho správce front migrovat z použití LTS kódu vydání na CD kód vydání nebo z použití CD kódu vydání na LTS kód vydání za předpokladu, že cílové vydání je vyšší než vydání používané před migrací.

Z produktu IBM MQ for z/OS 9.2.0můžete migrovat tam a zpět mezi verzemi produktu CD a LTS se stejným VRM tolikrát, kolikrát je potřeba, a to bez dopadu na schopnost zpětné migrace. Správce front lze například spustit na adrese IBM MQ for z/OS 9.3.0 LTS, poté vypnout a spustit na adrese IBM MQ for z/OS 9.3.0 CD, poté vypnout a spustit na adrese IBM MQ for z/OS 9.3.0 LTS.

Produkt IBM MQ for z/OS tradičně poskytuje náhradní schopnost (zpětná migrace), takže po období spuštění po migraci se můžete vrátit k předchozí verzi. Tato schopnost je zachována pro vydání LTS a ta vydání produktu CD s modifikátorem `0` , jako např. 9.3.0 CD, ale není možná, když je zdrojem nebo cílem migrace vydání produktu CD s nenulovým číslem modifikátoru, například 9.2.5 nebo 9.3.1.

Následují platné scénáře migrace a ilustrují, jak tento princip funguje:

Zdrojové vydání	Cílové vydání	Notes
9.0.0 LTS	9.3.0 LTS nebo 9.3.0 CD	Zpětná migrace není podporována, protože 9.0.0 LTS nemá standardní podporu.
9.1.0 LTS	9.3.0 LTS nebo 9.3.0 CD	Zpětná migrace je podporována.
9.2.0 LTS	9.3.0 LTS nebo 9.3.0 CD	Zpětná migrace je podporována.
9.2.5 CD	9.3.0 LTS nebo 9.3.0 CD	Zpětná migrace není podporována jako zdrojové vydání je CD s nenulovým modifikátorem.
9.3.0 LTS nebo 9.3.0 CD	9.3.1 CD	Zpětná migrace není podporována jako cílové vydání je CD s nenulovým modifikátorem. `Write to operator with reply` CSQY041D je vydán pro potvrzení migrace.

Související úlohy

Použití a odebrání údržby na z/OS

Související informace

Stažení produktu IBM MQ 9.3

IBM MQ a IBM MQ Appliance místní aspekty připravenosti na GDPR

Pro PID:

Distribuováno

- IBM MQ/IBM MQ Advanced - 5724-H72
- IBM MQ for HPE NonStop - 5724-A39

z/OS

- IBM MQ for z/OS - 5655-MQ9
- IBM MQ for z/OS Value Unit Edition - 5655-VU9
- IBM MQ Advanced for z/OS - 5655-AV9
- IBM MQ Advanced for z/OS Value Unit Edition - 5655-AV1

IBM MQ Appliance

- IBM MQ Appliance M2003 -5900-ALJ
- IBM MQ Appliance M2002 - 5737-H47

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 klienti budou v souladu s jakýmikoli 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 webové stránky

Konfigurace produktu-aspekty připravenosti na GDPR

Následující sekce poskytují pokyny pro konfiguraci produktu IBM MQ , které pomohou vaší organizaci s připraveností na GDPR.

Životní cyklus dat

Produkt IBM MQ je middlewarový produkt orientovaný na transakční zprávy, který umožňuje aplikacím asynchronně vyměňovat data poskytovaná aplikací. Produkt IBM MQ podporuje řadu rozhraní API systému zpráv, protokolů a mostů pro účely připojení aplikací. Jako takový může být IBM MQ použita k výměně mnoha forem dat, z nichž některé by mohly být předmětem GDPR. Existuje několik produktů třetích stran, se kterými si může produkt IBM MQ vyměňovat data. Některé z nich jsou vlastněny společností IBM, ale mnohé další jsou poskytovány 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 interaguje s daty, která jím procházejí, pomocí definice front, témat a odběrů.

Jaké typy datových toků IBM MQ?

Vzhledem k tomu, že produkt IBM MQ poskytuje asynchronní službu systému zpráv pro data aplikace, neexistuje žádná definitivní odpověď na tuto otázku, 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 se řídí nařízením 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. Data zpráv poskytnutá aplikací z/OS mohou být také zahrnuta do adresního prostoru nebo výpisů paměti prostředku Coupling Facility.

Níže jsou uvedeny některé typické příklady osobních údajů, které mohou být vyměněny pomocí IBM MQ:

- Zaměstnanci zákazníka (například IBM MQ může být použit pro připojení mzdových nebo personálních systémů zákazníka).
- Osobní údaje 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 CRM systému).
- Citlivé osobní údaje zákazníků (například IBM MQ mohou být použity v rámci odvětvových kontextů, které vyžadují výměnu osobních údajů, jako např. 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 o IBM MQ předmětech 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 produktu IBM Integration Ideas

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 údajů. Při posuzování vašeho používání IBM MQ a vašich potřeb vyhovět požadavkům GDPR byste měli zvážit typy osobních údajů, které za vašich okolností procházejí přes IBM MQ. 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 odkrýt aspekty dat zpráv aplikace procházejících produktem?)
- Jak jsou pověření shromažďována a ukládána v případě potřeby společností IBM MQ pro přístup k aplikacím třetích stran?

Produkt 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 správci front, produkt IBM MQ tato data přetrvají (možná více kopií) přímo na stavová média. Uživatelé produktu IBM MQ mohou zvážit zabezpečení dat zprávy v době, kdy jsou v klidu.

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

- Fronty zpráv aplikace:

  Produkt 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:

  Produkt IBM MQ Managed File Transfer využívá fronty zpráv ke koordinaci spolehlivého přenosu dat souboru, soubory obsahující osobní data a záznamy o přenosech jsou uloženy v těchto frontách.
- Přenosové fronty:

  Pro spolehlivý přenos zpráv mezi správci front jsou zprávy dočasně uloženy v přenosových frontách.
- Fronty nedoručených zpráv:

  Za určitých okolností nelze zprávy vkládat do cílové fronty a jsou uloženy ve frontě nedoručených zpráv, pokud je tato fronta konfigurována ve správci front.
- Fronty vrácení:

  Rozhraní systému zpráv JMS a XMS poskytují schopnost, která umožňuje přesunutí nezpracovatelných zpráv do fronty vrácení poté, co došlo k řadě vrácení, aby bylo možné zpracovat další platné zprávy.
- Fronta chyb AMS:

  Produkt IBM MQ Advanced Message Security přesune zprávy, které nejsou v souladu se zásadou zabezpečení, do systému SYSTEM.PROTECTION.ERROR.QUEUE je podobná frontě nedoručených zpráv.
- Zachovaná publikování:

  Produkt IBM MQ poskytuje zachovanou funkci publikování, která umožňuje odebírajícím aplikacím odvolat předchozí publikování.
- Odložené doručení:

Produkt IBM MQ podporuje funkci prodlevy doručení JMS 2.0 a Jakarta Messaging 3.0 , která umožňuje doručování zpráv do místa určení v budoucnosti. Zprávy, které dosud nebyly doručeny, jsou uloženy v systému SYSTEM.DDELAY.LOCAL.QUEUE .

Přečtěte si více:

- Protokolování: Ujistěte se, že zprávy nejsou ztraceny
- Nastavení fronty agenta MFT
- Použití fronty nedoručených zpráv
- Obsluha nezpracovatelných zpráv ve třídách IBM MQ pro JMS
- Ošetření chyb AMS
- Zachovaná publikování
- JMS 2.0 prodleva doručení

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

- Systém zpráv trasy trasování:

  Produkt IBM MQ poskytuje schopnosti trasovací 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:

  Produkt 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 k internímu kódu, kterými prochází datové toky zpráv. Jako součást těchto funkcí může produkt IBM MQ zaznamenat obsah dat zpráv poskytnutých aplikací do trasovacích souborů uložených na disku.
- Události správce front:

  Produkt IBM MQ může generovat zprávy událostí, které mohou zahrnovat osobní data, jako např. 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 and Linux® .
- 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.
- Omezte přístup k replikovaným kopiím dat IBM MQ v konfiguracích vysoké dostupnosti (HA) nebo zotavení z havárie (DR) a zabezpečte připojení používaná pro replikaci.
- Pomocí produktu IBM MQ Advanced Message Security můžete poskytovat komplexní podepisování a/nebo šifrování dat zpráv.
- Použijte šifrování na úrovni souboru nebo svazku k ochraně adresářů nebo systémů souborů, které mohou obsahovat data, trasování nebo protokoly systému IBM MQ .

- Po odeslání trasování služby do produktu IBMmůžete odstranit soubory trasování služby a data FFST, pokud máte obavy o obsah potenciálně obsahující osobní údaje.

Přečtěte si více:

- Oprávnění uživatelé
- Plánování podpory systému souborů na platformě Multiplatforms
- Šifrování systému souborů na serveru IBM MQ Appliance

Administrátor produktu IBM MQ může nakonfigurovat správce front s pověřeními (jméno uživatele a heslo, klíče rozhraní API atd.) pro služby 3rd stran, jako např. LDAP, Salesforceatd. 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. Administrátoři produktu IBM MQ jsou považováni za oprávněné uživatele a jsou členy této skupiny, takže mají k souborům přístup pro čtení. 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 and Linux .
- 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 možnost 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 Administrativní rozhraní REST API [pouze vzdálené]
- IBM MQ Rozhraní REST API systému zpráv [pouze vzdálené]
- MQI [Lokální a vzdálený]
- JMS [Lokální a vzdálený]
- XMS [Lokální a vzdálený]
- IBM MQ Telemetrie (MQTT) [pouze vzdálené]
- IBM MQ Light (AMQP) [pouze vzdálený]
- IBM MQ IMS [Pouze lokální]
- IBM MQ CICS bridge [pouze lokální]
- 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 PCF příkazy [lokální a vzdálené]
- IBM MQ Příkazy MQSC [Lokální a vzdálené]

- IBM MQ Explorer [Lokální a vzdálený]
- IBM MQ Uživatelské procedury [pouze lokální]
- IBM MQ Internet Pass-Thru [Pouze vzdálený]
- Red Hat® OpenShift® Monitorování (Prometheus) metrik (metriky jsou číselná data o statistice správce front)
- Deprecated Removed IBM Cloud Pak for Integration Integrace řídicího panelu operací, která odesílá data trasování vysoké úrovně do centrálního zdroje (pouzeCP4I). Všimněte si, že tato funkce je zamítnuta v produktu IBM MQ Operator 2.3.0a odebrána v produktu IBM MQ Operator 2.4.0.
- IBM MQ Appliance Sériová konzola [pouze lokální]
- IBM MQ Appliance SSH [pouze vzdálené]
- IBM MQ Appliance REST API [pouze vzdálené]
- IBM MQ Appliance Web UI [pouze vzdálené]
- V 9.3.3 IBM MQ Kafka Konektory (Kafka Connect) [lokální a vzdálené]

Tato 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 zasílání 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)
3. Token zabezpečení (JWT) pouze IBM MQ a pouze z IBM MQ 9.3.4

Pokud byla administrativní akce vyžádána ze vzdáleného připojení, pak se komunikace s produktem IBM MQ provádí 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 LTPA2 nebo token JWT).
6. Další vlastní zabezpečení (schopnost poskytovaná 3rd stranami)
7. Klíče SSH

Integrace produktu IBM MQs produktem IBM Cloud Pak for Integration přidává nový typ ověřování pro produkt IBM MQ Console: Single Sign-On s produktem Cloud Pak. (pouzeCP4I)

Mapování rolí:

Ve fázi mapování rolí mohou být pověření poskytnutá ve fázi ověřování mapována na alternativní identifikátor uživatele. Za předpokladu, že je povoleno pokračovat s mapovaným identifikátorem uživatele (například administrativní uživatelé mohou být blokováni pravidly ověřování kanálu), je mapované ID uživatele přeneseno do konečné fáze při autorizaci aktivit vůči prostředkům 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 tak, aby vytvářeal události konfigurace při vytvoření, změně nebo odstranění prostředku správce front.
3. Správce front IBM MQ lze konfigurovat tak, aby generoval událost oprávnění v případě, že pro prostředek selže kontrola autorizace.
4. Do protokolů chyb správce front se zapisují chybové zprávy označující, že se nezdařily kontroly autorizace.
5. Konzola IBM MQ Console zapíše zprávy auditu do svých protokolů při selhání ověření, kontroly autorizace nebo při vytvoření, spuštění, zastavení nebo odstranění správců front.
6. IBM MQ Appliance zapíše zprávy auditu do svých protokolů, aby zaznamenala přihlášení uživatelů a změny systému.

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

- 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.
- Oprávnění uživatelé produktu IBM MQ mají dostatečná oprávnění pro zakázané události, 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
- Použití protokolů chyb

Zpracování dat

Šifrování pomocí infrastruktury veřejných klíčů:

Síťová připojení k produktu IBM MQ můžete zabezpečit určením, že připojení používají protokol TLS, který může také poskytovat vzájemné ověření inicializační strany připojení.

Použití zařízení zabezpečení PKI, která jsou poskytována mechanizmy 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 k používání funkcí produktu 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 SSL a certifikátů k zabezpečení síťových připojení naleznete v následujících tématech v dokumentaci k produktu IBM MQ :

- Konfigurace zabezpečení TLS pro IBM MQ
- Přehled AMS

Odstranění dat

Produkt IBM MQ poskytuje příkazy a akce uživatelského rozhraní pro odstranění dat, která byla dodána do produktu. To znamená, že uživatelé produktu IBM MQ mohou v případě potřeby odstranit data, která se týkají konkrétních osob.

- Oblasti chování společnosti IBM MQ , které je třeba vzít v úvahu pro dodržování 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 a všech replikovaných kopií pro vysokou dostupnost nebo zotavení z havárie.
  - Odstraňte data uložená příkazy trasování služby tak, že odstraníte soubory v adresáři trasování.
  - Odstraňte data FFST uložená odstraněním souborů v adresáři chyb.
  - Odstranit adresní prostor a výpisy paměti prostředku Coupling Facility (na systému z/OS).
  - Odstraňte archivní, záložní nebo jiné kopie těchto dat.
- Oblasti chování společnosti IBM MQ , které je třeba zvážit pro dodržování GDPR
  - Data účtu a předvolby uložené produktem IBM MQ pro připojení ke správcům front a službám 3rd můžete odstranit odstraněním (včetně jejich archivu, zálohy 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 agenty IBM MQ Managed File Transfer , moduly protokolování 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 z produktu IBM MQ Appliance, včetně odkazu na tyto účty v souborech systémového protokolu.
    - IBM MQ Explorer metadata pracovního prostoru a nastavení Eclipse .
    - IBM MQ Explorer úložiště hesel, jak je uvedeno v Předvolbách hesla.
    - IBM MQ Konfigurační soubory konzoly a serveru mqweb.

- Konfigurační soubory dat připojení Salesforce .
- Konfigurační soubory dat připojení Blockchain .
- Konfigurační soubory a úložiště klíčů IBM MQ Internet Pass-Thru .

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 Console uživatelů a rolí

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 Appliance monitorování a vytváření sestav

Schopnost omezovat používání osobních údajů

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

Fronty zpráv systému IBM MQ 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 pomocí standardních funkcí systému zpráv IBM MQ přistupovat k datům zpráv nebo je upravovat.

Zpracování souborů

1. IBM MQ Managed File Transfer neprovádí skenování malwaru přenášených souborů. 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 produkt MFT přenese soubor a poté, co produkt MFT doručí soubor do vzdáleného koncového bodu.
2. Produkt IBM MQ Managed File Transfer neprovádí akce na základě typu MIME nebo přípony souboru. Produkt MFT přečte soubory a přenese bajty přesně tak, jak byly načteny ze vstupního souboru.

Architektury založené na jednom správci front

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

Před plánováním architektury IBM MQ se seznamte se základními koncepty produktu IBM MQ . Viz IBM MQ Technický přehled.

Řada možných architektur používajících jednoho správce front je popsána v následujících sekcích:

- “Jeden správce front s lokálními aplikacemi přistupujícími ke službě” na stránce 18
- “Jeden správce front se vzdálenými aplikacemi přistupujícími ke službě jako klienti” na stránce 18
- “Jeden správce front s konfigurací publikování/odběru” na stránce 18

Jeden správce front s lokálními aplikacemi přistupujícími ke službě

První architektura založená na jednom správci front spočívá v tom, že aplikace, které přistupují ke službě, jsou spuštěny ve stejném systému jako aplikace poskytující službu. Správce front IBM MQ poskytuje asynchronní komunikaci mezi aplikacemi požadujícími službu a aplikacemi poskytujícími službu. To znamená, že komunikace mezi aplikacemi může pokračovat i v případě, že jedna z aplikací je po delší dobu offline.

Jeden správce front se vzdálenými aplikacemi přistupujícími ke službě jako klienti

Druhá architektura založená na jednom 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 lze poskytnout více systémům prostřednictvím jednoho správce front.

Omezení této architektury spočívá v tom, že musí být k dispozici síťové připojení, aby mohla aplikace fungovat. Interakce mezi aplikací a správcem front prostřednictvím síťového připojení je synchronní.

Jeden správce front s konfigurací publikování/odběru

Alternativní architekturou používající jednoho správce front je použití konfigurace publikování/odběru. V systému zpráv publikování/odběru můžete oddělit poskytovatele informací od spotřebitelů těchto informací. To se liší od jednotlivých stylů systému zpráv v dříve popsaných architekturách, kde aplikace musí znát informace o cílové aplikaci, například název fronty, do které se mají vkládat zprávy. Pomocí produktu IBM MQ publikování/odběr odesílající aplikace publikuje zprávu s určeným tématem na základě předmětu informací. Produkt IBM MQ zpracovává distribuci zprávy do aplikací, které zaregistrovaly zájem o daný předmět prostřednictvím odběru. Přijímající aplikace také nemusí vědět nic o zdroji zpráv, aby je obdržely. Další informace naleznete v tématu Publikování/odběr zpráv a Příklad konfigurace publikování/odběru jednoho správce front.

Související pojmy

Úvod do produktu IBM MQ

Související úlohy

“Plánování architektury IBM MQ” na stránce 5
Při plánování prostředí IBM MQ zvažte podporu, kterou produkt IBM MQ poskytuje pro jednu a více architektur správců front a pro styly systému zpráv typu point-to-point a publikování/odběr. Také naplánujte své požadavky na prostředky a použití protokolovacích a zálohovacích zařízení.

Vytvoření a správa správců front na platformě Multiplatforms

Architektury založené na více správcích front

Pomocí technik distribuovaného řazení zpráv do front můžete vytvořit architekturu IBM MQ zahrnující konfiguraci a použití více správců front.

Před plánováním architektury IBM MQ se seznamte se základními koncepty produktu IBM MQ . Viz IBM MQ Technický přehled.

Architekturu IBM MQ lze změnit bez úprav 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. Alternativně se mohou aplikace přistupující ke službě připojovat jako klienti ke správci front, který poté poskytuje asynchronní přístup ke službě v jiném správci front.

Trasy, které spojují různé správce front a jejich fronty, jsou definovány pomocí technik distribuovaného řazení do 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.

Chcete-li získat přehled vysoké úrovně plánování sítě IBM MQ , prohlédněte si téma "Návrh distribuovaných sítí správců front" na stránce 20.

Informace o plánování kanálů pro architekturu IBM MQ naleznete v tématu IBM MQ techniky distribuovaného řazení do front.

Distribuovaná správa front umožňuje vytvářet a monitorovat komunikaci mezi správci front. Další informace o správě distribuovaných front naleznete v tématu Úvod do správy distribuovaných front.

Související úlohy

"Plánování architektury IBM MQ" na stránce 5
Při plánování prostředí IBM MQ zvažte podporu, kterou produkt IBM MQ poskytuje pro jednu a více architektur správců front a pro styly systému zpráv typu point-to-point a publikování/odběr. Také naplánujte své požadavky na prostředky a použití protokolovacích a zálohovacích zařízení.

Vytvoření a správa správců front na platformě Multiplatforms

Plánování distribuovaných front a klastrů

Můžete ručně připojit fronty, jejichž hostitelem je distribuovaný správce front, nebo můžete vytvořit klastr správců front a nechat produkt připojit správce front za vás. Chcete-li zvolit vhodnou topologii pro síť distribuovaného systému zpráv, musíte zvážit své požadavky na ruční řízení, velikost sítě, frekvenci změn, dostupnost a rozšiřitelnost.

Než začnete

Tato úloha předpokládá, že chápete, jaké sítě distribuovaného systému zpráv jsou a jak fungují. Technický přehled naleznete v tématu Distribuované fronty a klastry.

Informace o této úloze

Chcete-li vytvořit síť distribuovaného systému zpráv, můžete ručně nakonfigurovat kanály pro připojení front, jejichž hostitelem je jiný správce front, nebo můžete vytvořit klastr správců front. Klastrování umožňuje správcům front vzájemnou komunikaci bez nutnosti nastavovat další definice kanálů nebo definice vzdálených front, což zjednodušuje jejich konfiguraci a správu.

Chcete-li zvolit vhodnou topologii pro vaši distribuovanou síť publikování/odběru, musíte zvážit následující široké otázky:

- Kolik ruční kontroly potřebujete přes připojení ve vaší síti?
- Jak velká bude vaše síť?
- Jak bude dynamická?
- Jaké jsou vaše požadavky na dostupnost a rozšiřitelnost?

Procedura

- Zvažte, jakou ruční kontrolu potřebujete nad připojeními ve vaší síti.

  Pokud potřebujete pouze několik připojení, nebo pokud je třeba jednotlivá připojení velmi přesně definovat, měli byste pravděpodobně vytvořit síť ručně.

  Potřebujete-li více správců front, kteří spolu logicky souvisí, a kteří potřebují sdílet data a aplikace, měli byste zvážit jejich seskupování v klastru správců front.
- Odhadněte, jak velká musí být vaše síť.
  a) Odhadněte, kolik správců front potřebujete. Mějte na paměti, že fronty mohou být hostovány ve více než jednom správci front.

b) Pokud uvažujete o použití klastru, přidejte dva další správce front, kteří budou pracovat jako úplná úložiště.

U větších sítí může být ruční konfigurace a údržba připojení velmi časově náročná a měli byste zvážit použití klastru.

- Zvažte, jak dynamická bude síťová aktivita.

  Plán pro zaneprázdněné fronty, které mají být hostovány na výkonných správcích front.

  Pokud očekáváte, že fronty budou často vytvářeny a odstraňovány, zvažte použití klastru.
- Zvažte své požadavky na dostupnost a rozšiřitelnost.
  a) Rozhodněte, zda potřebujete zaručit vysokou dostupnost správců front. Pokud ano, odhadněte počet správců front, na které se tento požadavek vztahuje.
  b) Zvažte, zda jsou někteří z vašich správců front méně schopní než jiní.
  c) Zvažte, zda jsou komunikační odkazy na některé z vašich správců front křehčí než na jiné.
  d) Zvažte hostování front ve více správcích front.

  Ručně nakonfigurované sítě a klastry lze konfigurovat tak, aby byly vysoce dostupné a rozšiřitelné. Používáte-li klastr, musíte definovat dva další správce front jako úplná úložiště. Díky dvěma úplným úložištím je zajištěno, že klastr bude i nadále fungovat, pokud se jedno z úplných úložišť stane nedostupným. Ujistěte se, že správci front úplného úložiště jsou robustní, výkonní a mají dobrou síťovou konektivitu. Neplánujte používat správce front úplného úložiště pro žádnou jinou práci.
- Na základě těchto výpočtů můžete pomocí poskytnutých odkazů rozhodnout, zda chcete ručně konfigurovat připojení mezi správci front, nebo zda chcete použít klastr.

Jak pokračovat dále

Nyní jste připraveni nakonfigurovat síť distribuovaného systému zpráv.

Související úlohy

Konfigurace distribuovaných front

Konfigurace klastru správců front

Návrh distribuovaných sítí správců front

Produkt IBM MQ odesílá a přijímá data mezi aplikacemi a přes sítě pomocí správců front a kanálů. Plánování sítě zahrnuje definování požadavků na vytvoření rámce pro připojení těchto systémů přes síť.

Kanály mohou být vytvořeny mezi vaším systémem a jakýmkoli jiným systémem, se kterým potřebujete komunikovat. Kanály s více přechody lze vytvořit pro připojení k systémům, kde nemáte žádná přímá připojení. Připojení kanálu zpráv popsaná ve scénářích jsou zobrazena jako diagram sítě v souboru Obrázek 1 na stránce 21.

Potřebujete-li vytvořit kanály mezi systémy v různých fyzických sítích nebo kanály, které komunikují prostřednictvím brány firewall, může použití produktu IBM MQ Internet Pass-Thru zjednodušit konfiguraci. Další informace naleznete v tématu IBM MQ Internet Pass-Thru.

Názvy kanálů a přenosových front

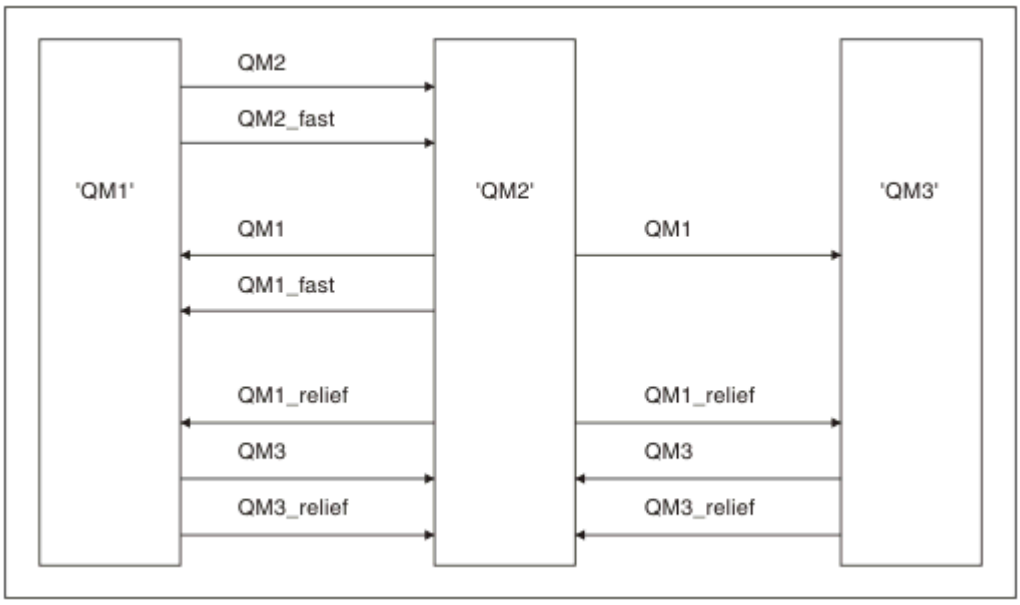
Přenosovým frontám lze zadat libovolný název. Chcete-li se však vyhnout nejasnostem, můžete jim podle potřeby přidělit stejné názvy jako názvy správců cílových front nebo názvy aliasů správců front. To přidruží přenosovou frontu k přenosové frontě, kterou používají, a poskytne jasný přehled paralelních tras vytvořených prostřednictvím intermediačních (vícepřechodových) správců front.

Pro názvy kanálů to není tak jasné. Například názvy kanálů v Obrázek 1 na stránce 21 pro QM2se musí lišit pro příchozí a odchozí kanály. Všechny názvy kanálů mohou stále obsahovat názvy přenosových front, ale musí být kvalifikovány tak, aby byly jedinečné.

Například v systému QM2je kanál QM3 pocházející z QM1a kanál QM3 je umístěn na QM3. Aby byly názvy jedinečné, první může mít název QM3_from_QM1a druhý může mít název QM3_from_QM2. Tímto

způsobem názvy kanálů zobrazují název přenosové fronty v první části názvu. Směr a název sousedního správce front jsou uvedeny v druhé části názvu.

Tabulka navržených názvů kanálů pro Obrázek 1 na stránce 21 je uvedena v souboru Tabulka 1 na stránce 21.



Obrázek 1. Síťový diagram zobrazující všechny kanály

Tabulka 1. Příklad názvů kanálů

Název trasy	**Hostitelský kanál správců front**	**Jméno přenosové fronty**	**Navrhovaný název kanálu**
QM1	QM1 & QM2	QM1 (na adrese QM2)	QM1.from.QM2
QM1	QM2 & QM3	QM1 (na QM3)	QM1.from.QM3
QM1_fast	QM1 & QM2	QM1_fast (v 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 adrese QM1)	QM2.from.QM1
QM2_fast	QM1 & QM2	QM2_fast (v QM1)	QM2_fast.from.QM1
QM3	QM1 & QM2	QM3 (v QM1)	QM3.from.QM1
QM3	QM2 & QM3	QM3 (v QM2)	QM3.from.QM2
QM3_relief	QM1 & QM2	QM3_relief (na QM1)	QM3_relief.from.QM1
QM3_relief	QM2 & QM3	QM3_relief (na QM2)	QM3_relief.from.QM2

Poznámka:

1. z/OS V systému IBM MQ for z/OSjsou názvy správců front omezeny na čtyři znaky.
2. Pojmenujte všechny kanály ve vaší síti jedinečně. Jak je uvedeno v části Tabulka 1 na stránce 21, je dobrým způsobem, jak to provést, zahrnutí názvů zdrojového a cílového správce front do názvu kanálu.

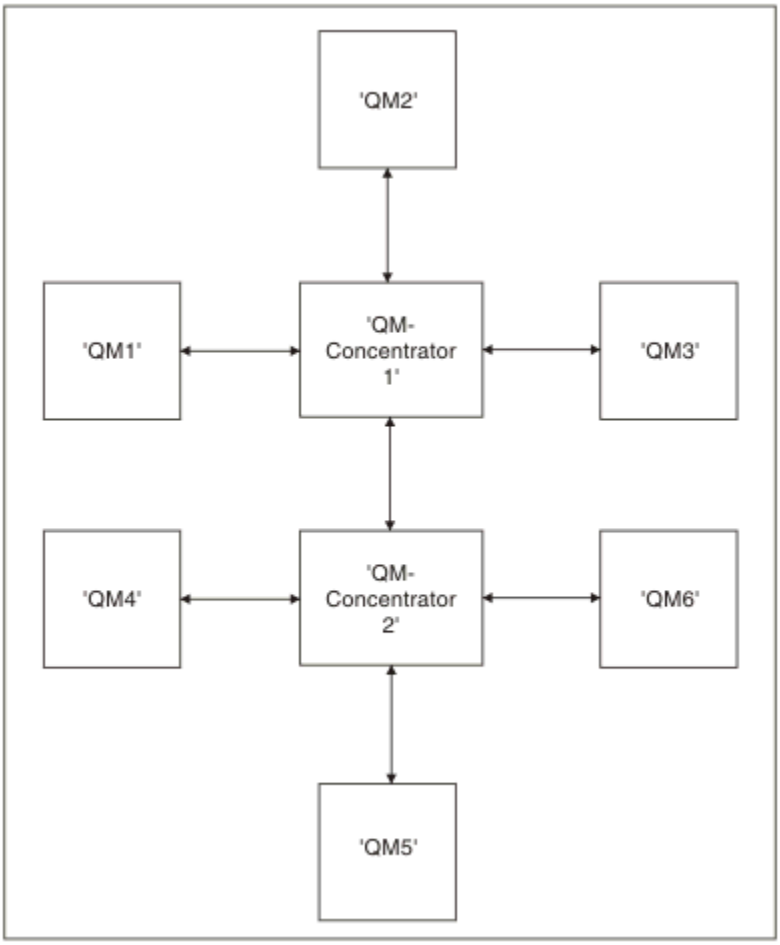
Plánovač sítě

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

Pro široce používané aplikace je hospodárnější přemýšlet o místních přístupových místech pro koncentraci přenosu zpráv pomocí širokoúhlých odkazů mezi lokálními přístupovými místy, jak je znázorněno v části Obrázek 2 na stránce 22.

V tomto příkladu jsou dva hlavní systémy a řada satelitních systémů. Skutečná konfigurace bude záviset na obchodních aspektech. V pohodlných centrech jsou umístěni dva správci front koncentrátoru. Každý koncentrátor QM má kanály zpráv pro lokální správce front:

- Koncentrátor QM 1 má kanály zpráv pro každého ze tří lokálních správců front, QM1, QM2a QM3. Aplikace používající tyto správce front mohou vzájemně komunikovat prostřednictvím koncentrátorů QM.
- Koncentrátor QM 2 má kanály zpráv pro každého ze tří lokálních správců front, QM4, QM5a QM6. Aplikace používající tyto správce front mohou vzájemně komunikovat prostřednictvím koncentrátorů QM.
- Koncentrátory QM mají mezi sebou kanály zpráv, což umožňuje jakékoli aplikaci ve správci front vyměňovat si zprávy s jakoukoli jinou aplikací v jiném správci front.



Obrázek 2. Síťový diagram zobrazující koncentrátory QM

Návrh klastrů

Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Klastry musí být pečlivě navrženy tak, aby zajistily, že budou správně fungovat a že dosáhnou požadované úrovně dostupnosti a schopnosti reagovat.

Než začnete

Úvod do koncepcí klastrování naleznete v následujících tématech:

- Distribuované fronty a klastry
- "Porovnání klastrování a distribuovaného řazení do front" na stránce 29
- Komponenty klastru

Při navrhování klastru správců front je třeba provést určitá rozhodnutí. Nejprve se musíte rozhodnout, kteří správci front v klastru mají uchovávat úplná úložiště informací o klastru. Každý správce front, kterého vytvoříte, může pracovat v klastru. Pro tento účel můžete zvolit libovolný počet správců front, ale ideální počet je dva. Informace o výběru správců front, kteří mají uchovávat úplná úložiště, naleznete v části "Jak vybrat správce front klastru pro uložení úplných úložišť" na stránce 31.

Další informace o návrhu klastru naleznete v následujících tématech:

- "Vzorové klastry" na stránce 37
- "Uspořádání klastru" na stránce 32
- "Konvence pojmenování klastrů" na stránce 33
- z/OS "Skupiny sdílení front a klastry" na stránce 34
- "Překrývající se klastry" na stránce 34

Jak pokračovat dále

Další informace o konfiguraci a práci s klastry naleznete v následujících tématech:

- Ustavení komunikace v klastru
- Konfigurace klastru správců front
- Směrování zpráv do klastrů a z klastrů
- Použití klastrů pro správu pracovní zátěže

Další informace, které vám pomohou s konfigurací klastru, viz"Rady pro klastrování" na stránce 35.

Plánování způsobu použití více přenosových front klastru

Můžete explicitně definovat přenosové fronty nebo nechat systém generovat přenosové fronty za vás.

Definujete-li přenosové fronty sami, máte větší kontrolu nad definicemi front. z/OS V systému z/OSmáte také větší kontrolu nad sadou stránek, kde jsou zprávy zadrženy.

Definování přenosových front

Existují dvě metody definování přenosových front:

- Automaticky pomocí atributu správce front DEFCLXQ:

  ```
  ALTER QMGR DEFCLXQ(SCTQ | CHANNEL)
  ```

  DEFCLXQ (SCTQ) označuje, že výchozí přenosová fronta pro všechny odesílací kanály klastru je SYSTEM.CLUSTER.TRANSMIT.QUEUE. Toto je výchozí hodnota.

  DEFCLXQ (CHANNEL) označuje, že standardně každý odesílací kanál klastru používá oddělenou přenosovou frontu s názvem SYSTEM.CLUSTER.TRANSMIT.*název kanálu*. Každá přenosová fronta je automaticky definována správcem front. Další informace viz "Automaticky definované přenosové fronty klastru" na stránce 25.
- Ručně, definováním přenosové fronty s hodnotou uvedenou pro atribut CLCHNAME. Atribut CLCHNAME označuje, které odesílací kanály klastru by měly používat přenosovou frontu. z/OS Pokud ručně definujete přenosovou frontu v systému z/OS, další informace viz "Plánování ručně definovaných přenosových front klastru" na stránce 26 .

Jakou bezpečnost potřebuji?

Chcete-li spustit přepínač, buď automaticky, nebo ručně, potřebujete oprávnění ke spuštění kanálu.

Chcete-li definovat frontu používanou jako přenosovou frontu, potřebujete k definování fronty standardní oprávnění IBM MQ .

Kdy je vhodný čas na provedení změny?

Při změně přenosové fronty používané odesílacími kanály klastru je třeba přidělit čas pro provedení aktualizace s ohledem na následující body:

- Doba, kterou kanál potřebuje k přepnutí přenosové fronty, závisí na celkovém počtu zpráv ve staré přenosové frontě, na počtu zpráv, které je třeba přesunout, a na velikosti zpráv.
- Aplikace mohou v průběhu změny nadále vkládat zprávy do přenosové fronty. To může vést k prodloužení doby přechodu.
- Parametr CLCHNAME libovolné přenosové fronty nebo DEFCLXQ můžete kdykoli změnit, pokud je pracovní zátěž nízká.

  Všimněte si, že se nic nestane okamžitě.
- Ke změnám dochází pouze při spuštění nebo restartování kanálu. Když se kanál spustí, zkontroluje aktuální konfiguraci a v případě potřeby se přepne na novou přenosovou frontu.
- Existuje několik změn, které mohou změnit přidružení odesílacího kanálu klastru k přenosové frontě:
  - Změna hodnoty atributu CLCHNAME přenosové fronty, což učiní CLCHNAME méně specifickým nebo prázdným.
  - Změna hodnoty atributu CLCHNAME přenosové fronty, což činí CLCHNAME specifičtější.
  - Odstranění fronty se zadaným CLCHNAME.
  - Změna atributu správce front DEFCLXQ.

Jak dlouho bude spínač trvat?

Během přechodného období jsou všechny zprávy pro kanál přesunuty z jedné přenosové fronty do jiné. Doba, kterou kanál potřebuje k přepnutí přenosové fronty, závisí na celkovém počtu zpráv ve staré přenosové frontě a na počtu zpráv, které je třeba přesunout.

Pro fronty obsahující několik tisíc zpráv by mělo přesunutí zpráv trvat méně než sekundu. Skutečný čas závisí na počtu a velikosti zpráv. Váš správce front by měl být schopen přesouvat zprávy v megabajtech za sekundu.

Aplikace mohou v průběhu změny nadále vkládat zprávy do přenosové fronty. To může vést k prodloužení doby přechodu.

Každý ovlivněný odesílací kanál klastru musí být restartován, aby se změna projevila. Proto je nejlepší změnit konfiguraci přenosové fronty, když není správce front zaneprázdněn, a v přenosových frontách klastru je uloženo několik zpráv.

Příkaz **runswchl** command z/OS nebo příkaz SWITCH CHANNEL (*) STATUS v CSQUTIL v systému z/OS, lze použít k dotazování na stav odesílacích kanálů klastru a na nevyřízené změny v konfiguraci přenosové fronty.

Jak implementovat změnu

Podrobnosti o tom, jak provádět změny ve více přenosových frontách klastru, a to buď automaticky, nebo ručně, naleznete v tématu Implementace systému pomocí více přenosových front klastru .

Zrušení změny

z/OS

Podrobné informace o tom, jak vrátit změny zpět, pokud narazíte na problémy, naleznete v tématu Vrátit zpět změnu přenosové fronty v systému z/OS .

Automaticky definované přenosové fronty klastru
Můžete nechat systém, aby za vás generoval přenosové fronty.

Než začnete

z/OS Chcete-li nastavit přenosové fronty klastru ručně v systému z/OS, prohlédněte si téma “Plánování ručně definovaných přenosových front klastru” na stránce 26.

Informace o této úloze

Pokud kanál nemá ručně definovanou přenosovou frontu klastru, která je k němu přidružena, a pokud zadáte hodnotu DEFCLXQ (CHANNEL), při spuštění kanálu správce front automaticky definuje trvalou dynamickou frontu pro odesílací kanál klastru. Modelová fronta SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE se používá k automatickému definování trvalé přenosové fronty dynamického klastru s názvem SYSTEM.CLUSTER.TRANSMIT.`ChannelName`.

Důležité: z/OS

Pokud je správce front migrován do adresáře IBM MQ 8.0, nemá tento správce front k dispozici systém SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE.

Nejprve definujte tuto frontu, aby se uplatil příkaz ALTER QGMR DEFCLXQ (CHANNEL).

Následující kód JCL je příkladem kódu, který můžete použít k definování modelové fronty:

```
//CLUSMODL JOB MSGCLASS=H,NOTIFY=&SYSUID
/*JOBPARM SYSAFF=(MVCC)
//MQCMD EXEC PGM=CSQUTIL,REGION=4096K,PARM='CDLK'
//STEPLIB DD DISP=SHR,DSN=SCEN.MQ.V000.COM.BASE.SCSQAUTH
// DD DISP=SHR,DSN=SCEN.MQ.V000.COM.BASE.SCSQANLE
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND DDNAME(CMDINP)
/*
//CMDINP DD *
DEFINE QMODEL( 'SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE' ) +
QSGDISP( QMGR ) +

* COMMON QUEUE ATTRIBUTES
DESCR( 'SYSTEM CLUSTERING TRANSMISSION MODEL QUEUE' ) +
PUT( ENABLED ) +
DEFPRTY( 5 ) +
DEFPSIST( YES ) +

* MODEL QUEUE ATTRIBUTES
DEFTYPE( PERMDYN ) +

* LOCAL QUEUE ATTRIBUTES
GET( ENABLED ) +
SHARE +
DEFSOPT( EXCL ) +
MSGDLVSQ( PRIORITY ) +
RETINTVL( 999999999 ) +
MAXDEPTH( 999999999 ) +
MAXMSGL( 4194304 ) +
NOHARDENBO +
BOTHRESH( 0 ) +
BOQNAME( ' ' ) +
STGCLASS( 'REMOTE' ) +
USAGE( XMITQ ) +
INDXTYPE( CORRELID ) +
CFSTRUCT( ' ' ) +
MONQ( OFF ) ACCTQ( OFF ) +

* EVENT CONTROL ATTRIBUTES
QDPMAXEV( ENABLED ) +
QDPHIEV( DISABLED ) +
QDEPTHHI( 80 ) +
QDPLOEV( DISABLED ) +
QDEPTHLO( 40 ) +
QSVCIEV( NONE ) +
QSVCINT( 999999999 ) +

* TRIGGER ATTRIBUTES
TRIGGER +
TRIGTYPE( FIRST ) +
TRIGMPRI( 0 ) +
TRIGDPTH( 1 ) +
TRIGDATA( ' ' ) +
PROCESS( ' ' ) +
INITQ( ' ' )
/*
```

Postup

1. Použijte atribut správce front *DEFCLXQ* .

   Další informace o tomto atributu viz ALTER QMGR.

   Existují dvě volby:

   Sctq
   Tato volba je výchozí a znamená, že používáte jediný SYSTEM.CLUSTER.TRANSMIT.QUEUE.

   CHANNEL
   Znamená, že používáte více přenosových front klastru.
2. Chcete-li přepnout na nové přidružení, postupujte takto:
   - Zastavte a restartujte kanál.
   - Kanál používá novou definici přenosové fronty.
   - Zprávy jsou přenášeny přechodným procesem přepnutí ze staré fronty do nové přenosové fronty.

   Všimněte si, že všechny zprávy aplikace jsou vloženy do staré definice.

   Když počet zpráv ve staré frontě dosáhne nuly, nové zprávy se umístí přímo do nové přenosové fronty.
3. Chcete-li sledovat, kdy proces přepínání skončí, postupujte takto:
   a) Přepínač přenosové fronty, který je iniciován kanálem, je spuštěn na pozadí a administrátor může monitorovat protokol úlohy správce front a určit, kdy byl dokončen.
   b) Monitorujte zprávy v protokolu úlohy, abyste zobrazili průběh přepínače.
   c) Chcete-li se ujistit, že tuto přenosovou frontu používají pouze požadované kanály, zadejte příkaz DIS CLUSQMGR (*), kde například vlastnost přenosové fronty, která definuje přenosovou frontu, je `APPQMGR.CLUSTER1.XMITQ`.
   d) z/OS
   Použijte příkaz SWITCH CHANNEL (*) STATUS pod CSQUTIL.

   Tato volba vám sděluje, jaké nevyřízené změny jsou nevyřízené a kolik zpráv je třeba přesunout mezi přenosovými frontami.

Výsledky

Nastavili jste přenosovou frontu klastru nebo fronty.

Související úlohy

“Plánování ručně definovaných přenosových front klastru” na stránce 26
Pokud v systému IBM MQ for z/OSdefinujete přenosové fronty sami, máte větší kontrolu nad definicemi a sadou stránek, na kterých jsou zprávy zadrženy.

Související odkazy

ALTER QMGR
ZOBRAZENÍ SOUBORU CLUSQMGR

z/OS *Plánování ručně definovaných přenosových front klastru*
Pokud v systému IBM MQ for z/OSdefinujete přenosové fronty sami, máte větší kontrolu nad definicemi a sadou stránek, na kterých jsou zprávy zadrženy.

Než začnete

Chcete-li nastavit přenosové fronty klastru automaticky, prohlédněte si téma “Automaticky definované přenosové fronty klastru” na stránce 25.

Informace o této úloze

Administrátor ručně definuje přenosovou frontu a pomocí atributu fronty CLCHNAME definuje, který odesílací kanál klastru nebo kanály budou tuto frontu používat jako svou přenosovou frontu.

Všimněte si, že CLCHNAME může obsahovat zástupný znak na začátku nebo na konci, aby bylo možné použít jednu frontu pro více kanálů.

Postup

1. Například zadejte následující příkaz:

```
DEFINE QLOCAL(APPQMGR.CLUSTER1.XMITQ)
CLCHNAME(CLUSTER1.TO.APPQMGR)
USAGE(XMITQ) STGCLASS(STG1)
INDXTYPE( CORRELID ) SHARE

DEFINE STGCLASS(STG1) PSID(3)
DEFINE PSID(3) BUFFERPOOL(4)
```

   Tip: Musíte naplánovat, kterou sadu stránek (a fond vyrovnávacích pamětí) použijete pro přenosové fronty. Můžete mít různé sady stránek pro různé fronty a poskytnout mezi nimi izolaci, takže jedno zaplnění sady stránek nebude mít vliv na přenosové fronty v jiných sadách stránek.

   Informace o tom, jak každý kanál vybírá odpovídající frontu, naleznete v tématu Práce s přenosovými frontami klastru a odesílacími kanály klastru .

   Když se kanál spustí, přepne své přidružení na novou přenosovou frontu. Aby nedošlo ke ztrátě žádné zprávy, správce front automaticky přenese zprávy ze staré přenosové fronty klastru do nové přenosové fronty v pořadí.
2. Použijte funkci CSQUTIL SWITCH pro změnu na nové přidružení.

   Další informace viz Přepnout přenosovou frontu přidruženou k odesílacím kanálům klastru (SWITCH) .

   a) STOP kanál nebo kanály, jejichž přenosová fronta má být změněna, aby byly ve stavu ZASTAVENO.

      Příklad:

```
STOP CHANNEL(CLUSTER1.TO.APPQMGR)
```

   b) Změňte atribut `CLCHNAME(XXXX)` v přenosové frontě.

   c) Pomocí funkce SWITCH můžete přepínat zprávy nebo sledovat, co se děje.

      Použít příkaz

```
SWITCH CHANNEL(*) MOVEMSGS(YES)
```

      přesunout zprávy bez spuštění kanálu.

   d) Spusťte kanál nebo kanály a zkontrolujte, zda kanál používá správné fronty.

      Příklad:

```
DIS CHS(CLUSTER1.TO.APPQMGR)
DIS CHS(*) where(XMITQ eq APPQMGR.CLUSTER1.XMITQ)
```

   Tip: Následující proces používá funkci CSQUTIL SWITCH. Další informace naleznete v tématu Přepnutí přenosové fronty přidružené k odesílacím kanálům klastru (SWITCH).

   Tuto funkci nemusíte používat, ale použití této funkce poskytuje více voleb:

   - Pomocí funkce SWITCH CHANNEL (*) STATUS lze snadno identifikovat stav přepínání odesílacích kanálů klastru. Umožňuje administrátorovi zjistit, které kanály aktuálně přepínají, a kanály s nevyřízeným přepínačem, které se projeví při příštím spuštění těchto kanálů.

Bez této funkce musí administrátor použít více příkazů DISPLAY a poté zpracovat výsledný výstup, aby tyto informace zjistil. Administrátor může také potvrdit, že změna konfigurace má požadovaný výsledek.

- Pokud se k inicializaci přepínače používá CSQUTIL, bude CSQUTIL i nadále monitorovat průběh této operace a skončí pouze po dokončení přepínače.

  To může výrazně usnadnit provádění těchto operací v dávce. Je-li také spuštěn CSQUTIL pro přepínání více kanálů, provede CSQUTIL tyto akce postupně; to může mít menší dopad na váš podnik než více paralelně spuštěných přepínačů.

Výsledky

Nastavili jste přenosovou frontu nebo fronty klastru v systému z/OS.

Řízení přístupu a více přenosových front klastru

Zvolte mezi třemi režimy kontroly, když aplikace vkládá zprávy do vzdálených front klastru. Režimy vzdáleně kontrolují frontu klastru, lokálně kontrolují produkt SYSTEM.CLUSTER.TRANSMIT.QUEUEnebo lokální profily pro frontu klastru nebo správce front klastru.

Produkt IBM MQ vám dává možnost lokálně nebo lokálně a vzdáleně zkontrolovat, zda má uživatel oprávnění vložit zprávu do vzdálené fronty. Typická aplikace IBM MQ používá pouze lokální kontrolu a spoléhá na vzdáleného správce front, který důvěřuje kontrolám přístupu provedeným v lokálním správci front. Pokud se nepoužije vzdálená kontrola, zpráva se vloží do cílové fronty s oprávněním procesu vzdáleného kanálu zpráv. Chcete-li použít vzdálenou kontrolu, musíte nastavit oprávnění vložení přijímacího kanálu na zabezpečení kontextu.

Lokální kontroly jsou prováděny pro frontu, kterou aplikace otevře. V distribuovaném řazení do front aplikace obvykle otevře definici vzdálené fronty a provede se kontrola přístupu vůči definici vzdálené fronty. Je-li zpráva vložena s úplným záhlavím směrování, budou provedeny kontroly přenosové fronty. Pokud aplikace otevře frontu klastru, která není v lokálním správci front, neexistuje žádný lokální objekt, který by bylo možné zkontrolovat. Kontroly řízení přístupu se provádějí pro přenosovou frontu klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE. I s více přenosovými frontami klastru jsou provedeny lokální kontroly řízení přístupu pro fronty vzdáleného klastru vůči produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Volba lokální nebo vzdálené kontroly je volba mezi dvěma extrémy. Kontrola na dálku je jemná. Každý uživatel musí mít profil řízení přístupu v každém správci front v klastru, aby jej mohl vložit do libovolné fronty klastru. Lokální kontrola je hrubozrnná. Každý uživatel potřebuje pro přenosovou frontu klastru ve správci front, ke kterému je připojen, pouze jeden profil řízení přístupu. Pomocí tohoto profilu mohou vložit zprávu do libovolné fronty klastru v libovolném správci front v libovolném klastru.

Administrátoři mají jiný způsob, jak nastavit řízení přístupu pro fronty klastru. Můžete vytvořit profil zabezpečení pro frontu klastru v libovolném správci front v klastru pomocí příkazu **setmqaut** . Profil se projeví, pokud otevřete vzdálenou frontu klastru lokálně a zadáte pouze název fronty. Můžete také nastavit profil pro vzdáleného správce front. Pokud tak učiníte, může správce front zkontrolovat profil uživatele, který otevře frontu klastru, zadáním úplného názvu.

Nové profily fungují pouze v případě, že změníte sekci správce front **ClusterQueueAccessControl** na RQMName. Výchozí hodnota je Xmitq. Musíte vytvořit profily pro všechny fronty klastru, které existující aplikace používají fronty klastru. Pokud změníte sekci na RQMName bez vytvoření profilů, aplikace pravděpodobně selžou.

Tip: Kontrola přístupu ke frontě klastru se nevztahuje na vzdálené řazení do fronty. Kontroly přístupu jsou stále prováděny vůči lokálním definicím. Změny znamenají, že při konfiguraci kontroly přístupu ve frontách klastru a tématech klastru můžete postupovat stejně. z/OS Změny také lépe zarovnají přístup ke kontrole přístupu pro fronty klastru s z/OS. Příkazy pro nastavení kontroly přístupu v systému z/OS se liší, ale oba tyto příkazy kontrolují přístup k profilu spíše než k objektu samotnému.

Související pojmy

“Klastrování: Izolace aplikace pomocí více přenosových front klastru” na stránce 45

Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášené různými odesílacími kanály klastru můžete umístit do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma poskytuje příklady a některé doporučené postupy, které vás provedou výběrem přístupu k použití.

Související úlohy

Nastavení `ClusterQueueAccessControl`

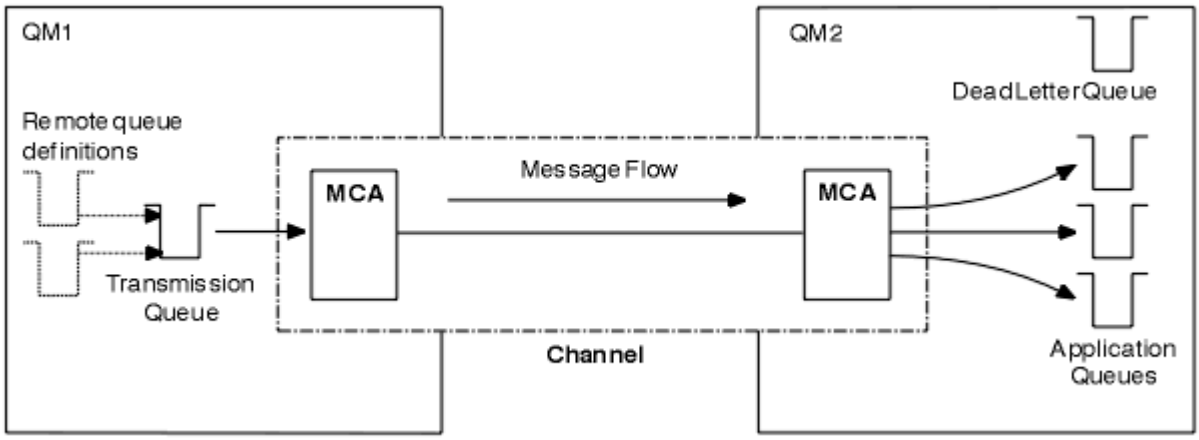
Porovnání klastrování a distribuovaného řazení do front

Porovnejte komponenty, které je třeba definovat pro připojení správců front pomocí distribuovaného řazení do front a klastrování.

Pokud nepoužíváte klastry, jsou vaši správci front nezávislí a komunikují pomocí distribuovaného řazení do front. Pokud jeden správce front potřebuje odeslat zprávy jinému správci front, musíte definovat:

- Přenosová fronta
- Kanál pro vzdáleného správce front

Obrázek 3 na stránce 29 zobrazuje komponenty požadované pro distribuované řazení do front.



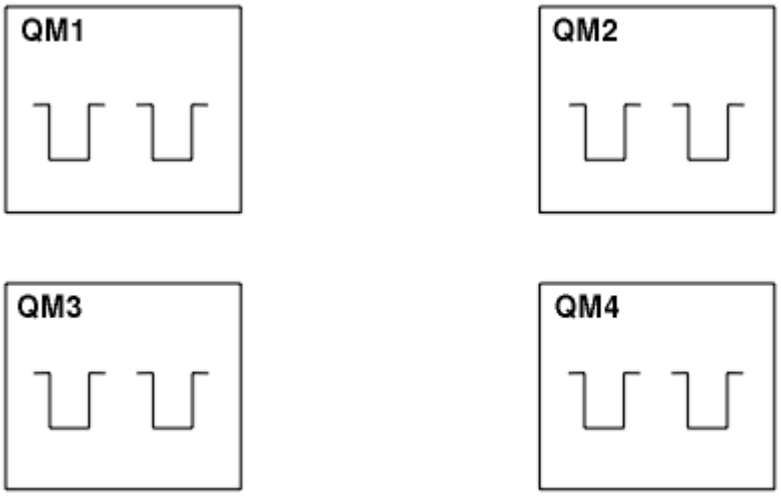
Obrázek 3. distribuované fronty

Pokud seskupíte správce front v klastru, budou fronty v libovolném správci front k dispozici všem ostatním správcům front v klastru. Kterýkoli správce front může odeslat zprávu jinému správci front ve stejném klastru bez explicitních definic. Pro každé místo určení neposkytujete definice kanálů, definice vzdálených front ani přenosové fronty. Každý správce front v klastru má jednu přenosovou frontu, ze které může přenášet zprávy do libovolného jiného správce front v klastru. Každý správce front v klastru musí definovat pouze:

- Jeden přijímací kanál klastru, na kterém mají být přijímány zprávy.
- Jeden odesílací kanál klastru, se kterým se představí a dozví se o klastru.

Definice pro nastavení klastru a distribuovaného řazení do front

Podívejte se na soubor Obrázek 4 na stránce 30, který zobrazuje čtyři správce front se dvěma frontami. Zvažte, kolik definic je potřeba pro připojení těchto správců front pomocí distribuovaných front. Porovnejte, kolik definic je potřeba k nastavení stejné sítě jako klastr.



Obrázek 4. Síť čtyř správců front

Definice pro nastavení sítě pomocí distribuovaného řazení do front

Chcete-li nastavit síť zobrazenou v produktu Obrázek 3 na stránce 29 pomocí distribuovaného řazení do front, můžete mít následující definice:

Tabulka 2. Definice pro distribuované řazení do front

Popis	**Počet na jednoho správce front**	**Celkový počet**
Definice odesílacího kanálu pro kanál, v němž mají být odesílány zprávy všem ostatním správcům front.	3	12
Definice přijímacího kanálu pro kanál, v němž mají být přijímány zprávy od všech ostatních správců front.	3	12
Definice přenosové fronty pro přenosovou frontu pro všechny ostatní správce front.	3	12
Definice lokální fronty pro každou lokální frontu.	2	8
Definice vzdálené fronty pro každou vzdálenou frontu, do které chce tento správce front vkládat zprávy.	6	24

Tento počet definic můžete snížit pomocí generických definic přijímacích kanálů. Maximální počet definic může být v každém správci front až 17, což je pro tuto síť celkem 68.

Definice pro nastavení sítě pomocí klastrů

Chcete-li nastavit síť zobrazenou v produktu Obrázek 3 na stránce 29 pomocí klastrů, potřebujete následující definice:

Tabulka 3. Definice pro klastrování

Popis	**Počet na jednoho správce front**	**Celkový počet**
Definice odesílacího kanálu klastru pro kanál, v němž mají být odesílány zprávy správci front úložiště.	1	4

Tabulka 3. Definice pro klastrování (pokračování)		
Popis	**Počet na jednoho správce front**	**Celkový počet**
Definice přijímacího kanálu klastru pro kanál, v němž mají být přijímány zprávy od jiných správců front v klastru.	1	4
Definice lokální fronty pro každou lokální frontu.	2	8

Chcete-li nastavit tento klastr správců front (se dvěma úplnými úložišti), potřebujete pro každého správce front čtyři definice, celkem šestnáct definic. Dále je třeba změnit definice správců front pro dva ze správců front tak, aby byly správci front úplného úložiště pro klastr.

Je vyžadována pouze jedna definice kanálu CLUSSDR a jedna definice kanálu CLUSRCVR . Je-li klastr definován, můžete přidat nebo odebrat správce front (jiné než správce front úložiště) bez narušení ostatních správců front.

Použití klastru snižuje počet definic potřebných k nastavení sítě obsahující mnoho správců front.

S menším počtem definic, které je třeba definovat, existuje menší riziko chyb:

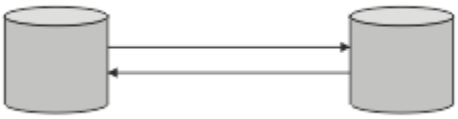
- Názvy objektů se vždy shodují, například název kanálu ve dvojici odesilatel-příjemce.
- Název přenosové fronty uvedený v definici kanálu vždy odpovídá správné definici přenosové fronty nebo názvu přenosové fronty uvedenému v definici vzdálené fronty.
- Definice QREMOTE vždy ukazuje na správnou frontu ve vzdáleném správci front.

Jakmile je klastr nastaven, můžete přesunout fronty klastru z jednoho správce front do jiného v rámci klastru, aniž byste museli provádět žádnou práci správy systému na jiném správci front. Není možné zapomenout na odstranění nebo úpravu definic kanálů, vzdálených front nebo přenosových front. Do klastru můžete přidávat nové správce front bez narušení stávající sítě.

Jak vybrat správce front klastru pro uložení úplných úložišť

V každém klastru musíte vybrat alespoň jednoho a nejlépe dva správce front, který bude obsahovat úplná úložiště. Dvě úplná úložiště jsou dostatečná pro všechny kromě těch nejvýjimečnějších okolností. Pokud je to možné, vyberte správce front, kteří jsou hostováni na robustních a trvale připojených platformách, kteří nemají výpadky, a kteří jsou geograficky na centrální pozici. Také zvažte vyhradit systémy jako hostitele úplného úložiště a nepoužívat tyto systémy pro žádné jiné úlohy.

Úplná úložiště jsou správci front, kteří udržují úplný obraz stavu klastru. Chcete-li tyto informace sdílet, je každé úplné úložiště připojeno kanály CLUSSDR (a jejich odpovídajícími definicemi CLUSRCVR) ke všem ostatním úplným úložištím v klastru. Tyto kanály musíte definovat ručně.



Obrázek 5. Dvě připojená úplná úložiště.

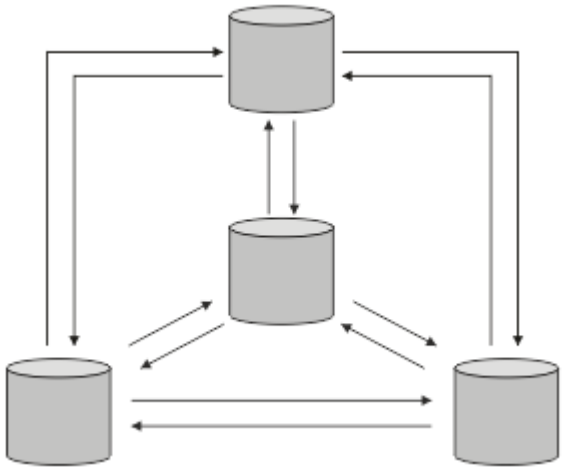
Každý jiný správce front v klastru udržuje obraz toho, co aktuálně ví o stavu klastru v *částečném úložišti*. Tito správci front publikují informace o sobě a vyžádají si informace o jiných správcích front pomocí libovolných dvou dostupných úplných úložišť. Není-li vybrané úplné úložiště k dispozici, použije se jiné. Když se znovu zpřístupní vybrané úplné úložiště, shromáždí nejnovější nové a změněné informace od ostatních, aby se udržely v kroku. Pokud jsou všechna úplná úložiště mimo provoz, ostatní správci front použijí informace, které mají ve svých dílčích úložištích. Jsou však omezeny na použití informací, které mají k dispozici; nové informace a žádosti o aktualizace nelze zpracovat. Když se úplná úložiště znovu připojují k síti, vyměňují se zprávy, aby byla všechna úložiště (úplná i částečná) aktuální.

Při plánování přidělení úplných úložišť je třeba vzít v úvahu následující aspekty:

- Správci front vybraní pro uložení úplných úložišť musí být spolehliví a spravovaní. Vyberte správce front, jejichž hostitelem je robustní a trvale připojená platforma.
- Zvažte plánované výpadky pro systémy, které hostují vaše úplná úložiště, a ujistěte se, že nemají shodující se výpadky.
- Zvažte výkon sítě: Vyberte správce front, kteří jsou geograficky na centrální pozici, nebo kteří sdílejí stejný systém jako ostatní správci front v klastru.
- Zvažte, zda je správce front členem více než jednoho klastru. Administrativně může být vhodné použít stejného správce front k hostování úplných úložišť pro několik klastrů za předpokladu, že tento přínos je v rovnováze s tím, jak očekáváte, že bude správce front zaneprázdněn.
- Zvažte vyhradit některé systémy tak, aby obsahovaly pouze úplná úložiště, a nepoužívat tyto systémy pro žádné jiné úlohy. To zajišťuje, že tyto systémy vyžadují údržbu pouze pro konfiguraci správce front a nejsou odebrány ze služby pro údržbu jiných obchodních aplikací. Také zajišťuje, aby úloha údržby úložiště nekonkurovala aplikacím pro systémové prostředky. To může být výhodné zejména ve velkých klastrech (například v klastrech s více než tisíci správci front), kde plná úložiště mají mnohem vyšší pracovní zátěž při udržování stavu klastru.

Je možné mít více než dvě úplná úložiště, ale zřídka doporučená. Ačkoli definice objektů (tj. fronty, témata a kanály) směřují do všech dostupných úplných úložišť, požadavky směřují pouze z částečného úložiště do maximálně dvou úplných úložišť. To znamená, že pokud jsou definována více než dvě úplná úložiště a jakákoli dvě úplná úložiště se stanou nedostupná, některá dílčí úložiště nemusí přijímat aktualizace, které by očekávala. Viz MQ Klastry: Proč pouze dvě úplná úložiště?

Jednou ze situací, v níž může být užitečné definovat více než dvě úplná úložiště, je migrace existujících úplných úložišť na nový hardware nebo nové správce front. V tomto případě byste měli před odebráním předchozích úplných úložišť zavést náhradní úplná úložiště a potvrdit, že byla naplněna daty. Kdykoli přidáte úplné úložiště, nezapomeňte, že jej musíte přímo připojit ke všem ostatním úplným úložištím pomocí kanálů CLUSSDR .



Obrázek 6. Více než dvě připojená úplná úložiště

Související informace

MQ Klastry: Proč pouze dvě úplná úložiště?
Jak velký může být klastr MQ ?

Uspořádání klastru

Vyberte, kteří správci front mají být propojeni s úplným úložištěm. Zvažte vliv výkonu, verzi správce front a zda je žádoucí více kanálů CLUSSDR .

Po výběru správců front, kteří mají uchovávat úplná úložiště, je třeba rozhodnout, kteří správci front mají být propojeni se kterým úplným úložištěm. Definice kanálu CLUSSDR propojuje správce front s úplným úložištěm, ze kterého zjišťuje další úplná úložiště v klastru. Od té doby správce front odesílá zprávy do libovolných dvou úplných úložišť. Vždy se pokusí použít ten, pro který má nejprve definici kanálu

CLUSSDR . Můžete se rozhodnout propojit správce front s úplným úložištěm. Při výběru zvažte topologii vaší konfigurace a fyzické nebo geografické umístění správců front.

Vzhledem k tomu, že všechny informace o klastru jsou odesílány do dvou úplných úložišť, může dojít k situacím, kdy chcete vytvořit druhou definici kanálu CLUSSDR . Můžete definovat druhý kanál CLUSSDR v klastru, který má mnoho úplných úložišť rozmístěných v široké oblasti. Poté můžete určit, do kterých dvou úplných úložišť jsou vaše informace odesílány.

Konvence pojmenování klastrů

Zvažte pojmenování správců front ve stejném klastru pomocí konvence pojmenování, která identifikuje klastr, do kterého správce front patří. Použijte podobnou konvenci pojmenování pro názvy kanálů a rozšiřte ji tak, aby popisovala charakteristiku kanálu.

Doporučené postupy při pojmenování klastrů produktu MQ

Ačkoli názvy klastrů mohou mít až 48 znaků, při použití konvencí pojmenování na jiné objekty jsou užitečné poměrně krátké názvy klastrů. Viz “Doporučené postupy při výběru názvů kanálů klastru” na stránce 33.

Při výběru názvu klastru je obvykle užitečné reprezentovat 'účel' klastru (který bude pravděpodobně dlouhý), spíše než 'obsah'. Například 'B2BPROD' nebo 'ACTTEST' spíše než 'QM1_QM2_QM3_CLUS'.

Doporučené postupy při výběru názvů správců front klastru

Vytváříte-li nový klastr a jeho členy od začátku, zvažte konvenci pojmenování pro správce front, která odráží jejich využití v klastru. Každý správce front musí mít jiný název. Správcům front v klastru však můžete poskytnout sadu podobných názvů, které vám pomohou identifikovat a zapamatovat si logická seskupení (například 'ACTTQM1, ACTTQM2).

Relativně krátké názvy správců front (například méně než 8 znaků) pomáhají, pokud se rozhodnete použít konvenci popsanou v další části nebo něco podobného pro názvy kanálů.

Doporučené postupy při výběru názvů kanálů klastru

Vzhledem k tomu, že správci front a klastry mohou mít názvy až 48 znaků a název kanálu je omezen na 20 znaků, dávejte pozor při prvním pojmenování objektů, abyste nemuseli měnit konvenci pojmenování v průběhu projektu (viz předchozí část).

Při definování kanálů mějte na paměti, že automaticky vytvořené odesílací kanály klastru ve všech správcích front v klastru přebírá své jméno z odpovídajícího přijímacího kanálu klastru konfigurovaného v přijímajícím správci front v klastru, a proto musí být tyto kanály jedinečné a musí mít smysl *ve vzdálených správcích front v klastru.*

Jedním z běžných přístupů je použít název správce front, kterému předchází název klastru. Pokud je například název klastru CLUSTER1 a správci front jsou QM1, QM2, pak jsou přijímací kanály klastru CLUSTER1.QM1, CLUSTER1.QM2.

Tuto konvenci můžete rozšířit, pokud mají kanály různé priority nebo používají různé protokoly. Příklad:

- CLUSTER1.QM1.S1
- CLUSTER1.QM1.N3
- CLUSTER1.QM1.T4

V tomto příkladu může být S1 prvním kanálem SNA, N3 může být kanálem NetBIOS s prioritou sítě tři a T4 může být TCP IP používající síť IPV4 .

Pojmenování definic sdílených kanálů

Jednu definici kanálu lze sdílet ve více klastrech. V takovém případě by zde navržené konvence pojmenování vyžadovaly úpravu. Jak je však popsáno v tématu Správa definic kanálů , je obvykle vhodnější definovat pro každý klastr v každém případě samostatné kanály.

Starší konvence pojmenování kanálů

Mimo klastrovaná prostředí bylo historicky běžné používat konvenci pojmenování 'FROMQM.TO.TARGETQM', takže můžete zjistit, že existující klastry použily něco podobného (například CLUSTER.TO.TARGET). Toto se nedoporučuje jako součást nového schématu pojmenování klastru, protože dále snižuje počet dostupných znaků, aby se v názvu kanálu předávaly 'užitečné' informace.

z/OS Názvy kanálů v systému IBM MQ for z/OS

Můžete definovat generické prostředky VTAM nebo generické názvy *Dynamic Domain Name Server* (DDNS). Názvy připojení můžete definovat pomocí generických názvů. Při vytváření definice příjemce klastru však nepoužívejte generický název připojení.

Problém s použitím generických názvů připojení pro definice příjemce klastru je následující: Pokud definujete CLUSRCVR s generickým CONNAME , není zaručeno, že vaše kanály CLUSSDR budou odkazovat na správce front, které zamýšlíte. Počáteční CLUSSDR může nakonec ukazovat na libovolného správce front ve skupině sdílení front, nikoli nutně na toho, který je hostitelem úplného úložiště. Pokud se kanál znovu spustí při pokusu o připojení, může se znovu připojit k jinému správci front se stejným generickým názvem a narušit tok zpráv.

z/OS *Skupiny sdílení front a klastry*

Sdílené fronty mohou být frontami klastru a správci front ve skupině sdílení front mohou být také správci front klastru.

V systému IBM MQ for z/OS můžete seskupit správce front do skupin sdílení front. Správce front ve skupině sdílení front může definovat lokální frontu, kterou má sdílet až 32 správců front.

Sdílené fronty mohou být také frontami klastru. Dále mohou být správci front ve skupině sdílení front také v jednom či více klastrech.

Můžete definovat generické prostředky VTAM nebo generické názvy *Dynamic Domain Name Server* (DDNS). Názvy připojení můžete definovat pomocí generických názvů. Při vytváření definice příjemce klastru však nepoužívejte generický název připojení.

Problém s použitím generických názvů připojení pro definice příjemce klastru je následující: Pokud definujete CLUSRCVR s generickým CONNAME , není zaručeno, že vaše kanály CLUSSDR budou odkazovat na správce front, které zamýšlíte. Počáteční CLUSSDR může nakonec ukazovat na libovolného správce front ve skupině sdílení front, nikoli nutně na toho, který je hostitelem úplného úložiště. Pokud se kanál znovu spustí při pokusu o připojení, může se znovu připojit k jinému správci front se stejným generickým názvem a narušit tok zpráv.

Kanál CLUSRCVR , který používá port modulu listener skupiny, nelze spustit, protože v takovém případě by nebylo možné určit, ke kterému správci front se má CLUSRCVR pokaždé připojit. Systémové fronty klastru, ve kterých jsou uchovávány informace o klastru, nejsou sdílené. Každý správce front má svůj vlastní.

Kanály klastru se používají nejen k přenosu zpráv aplikace, ale i interních systémových zpráv o nastavení klastru. Každý správce front v klastru musí obdržet tyto interní systémové zprávy, aby se správně podílel na klastrování, takže potřebuje vlastní jedinečný kanál CLUSRCVR , na kterém je obdrží.

Sdílený soubor CLUSRCVR může být spuštěn v libovolném správci front ve skupině sdílení front (QSG), a proto může vést k nekonzistentnímu dodání interních systémových zpráv správcům front skupiny QSG, což znamená, že se žádný nemůže řádně účastnit klastru. Chcete-li se ujistit, že nelze použít žádné sdílené kanály CLUSRCVR , jakýkoli pokus selže se zprávou CSQX502E .

Překrývající se klastry

Překrývající se klastry poskytují další administrativní schopnosti. Pomocí seznamů názvů snižte počet příkazů potřebných pro správu překrývajících se klastrů.

Můžete vytvořit klastry, které se překrývají. Existuje řada příčin, proč můžete definovat překrývající se klastry; například:

- Umožnit různým organizacím mít vlastní správu.
- Umožnit samostatnou správu nezávislých aplikací.

- Chcete-li vytvořit provozní třídy.

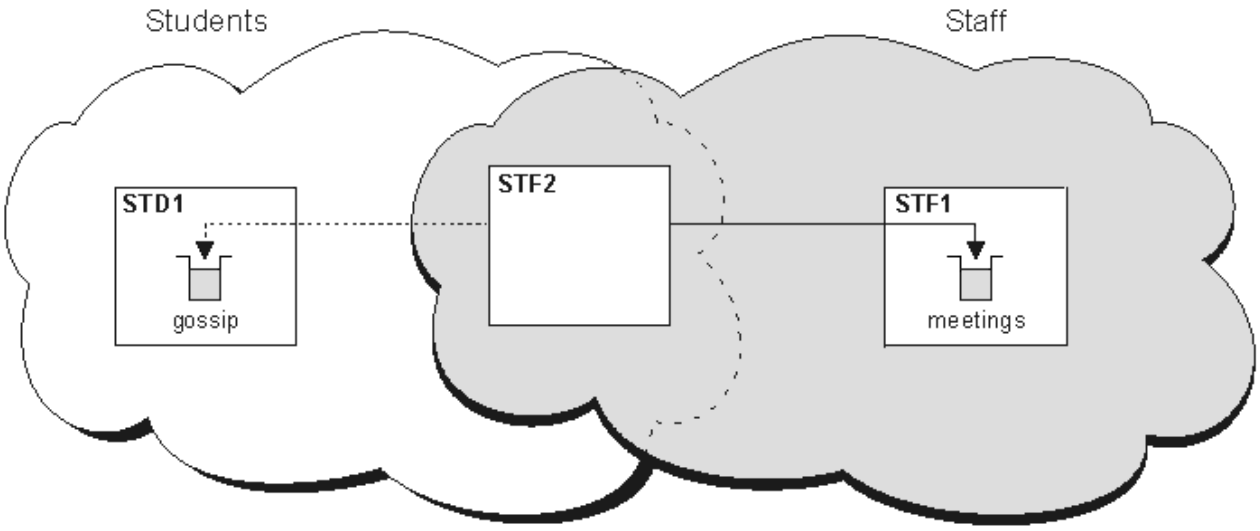
V produktu Obrázek 7 na stránce 35je správce front STF2 členem obou klastrů. Je-li správce front členem více než jednoho klastru, můžete využít seznamy názvů ke snížení počtu definic, které potřebujete. Seznamy názvů obsahují seznam názvů, například názvy klastrů. Můžete vytvořit seznam názvů, který bude pojmenovávat klastry. Zadejte seznam názvů v příkazu `ALTER QMGR` pro `STF2` , abyste z něj udělali správce front úplného úložiště pro oba klastry.

Máte-li v síti více než jeden klastr, musíte jim dát různé názvy. Pokud jsou dva klastry se stejným názvem sloučeny, není možné je znovu oddělit. Je také dobré dát klastrům a kanálům různá jména. Jsou snadněji rozlišitelné, když se podíváte na výstup z příkazů `DISPLAY` . Názvy správců front musí být v rámci klastru jedinečné, aby správně fungovaly.

Definování provozních tříd

Představte si univerzitu, která má správce front pro každého zaměstnance a každého studenta. Zprávy mezi zaměstnanci mají cestovat na kanálech s vysokou prioritou a vysokou šířkou pásma. Zprávy mezi studenty jsou cestovat na levnější, pomalejší kanály. Tuto síť můžete nastavit pomocí tradičních technik distribuovaného řazení do front. Produkt IBM MQ vybírá kanály, které mají být použity, podle názvu cílové fronty a názvu správce front.

Chcete-li jasně rozlišovat mezi zaměstnanci a studenty, můžete seskupit jejich správce front do dvou klastrů, jak ukazuje Obrázek 7 na stránce 35. Produkt IBM MQ přesouvá zprávy do fronty schůzek v klastru personálu pouze přes kanály definované v tomto klastru. Zprávy pro frontu protokolu Gossip v klastru studentů jdou přes kanály definované v tomto klastru a obdrží příslušnou provozní třídu.



Obrázek 7. Provozní třídy

Rady pro klastrování

Před použitím klastrování budete možná muset provést některé změny ve svých systémech nebo aplikacích. Existují jak podobnosti, tak rozdíly v chování distribuovaných front.

- Musíte přidat definice ruční konfigurace ke správcům front mimo klastr, aby mohli přistupovat k frontám klastrů.
- Pokud sloučíte dva klastry se stejným názvem, nemůžete je znovu oddělit. Proto je vhodné dát všem klastrům jedinečný název.
- Pokud zpráva dorazí do správce front, ale není zde žádná fronta, která by ji přijímala, je zpráva vložena do fronty nedoručených zpráv. Pokud neexistuje žádná fronta nedoručených zpráv, kanál selže a pokusí se znovu. Použití fronty nedoručených zpráv je stejné jako u distribuovaných front.
- Integrita trvalých zpráv je zachována. Zprávy nejsou duplikovány nebo ztraceny v důsledku použití klastrů.

- Použití klastrů snižuje administraci systému. Klastry usnadňují připojení větších sítí s mnoha více správci front, než byste byli schopni uvažovat pomocí distribuovaného řazení do front. Pokud se pokusíte povolit komunikaci mezi jednotlivými správci front v klastru, existuje riziko, že budete potřebovat nadměrné síťové prostředky.
- Používáte-li produkt IBM MQ Explorer, který prezentuje správce front ve stromové struktuře, může být zobrazení pro velké klastry těžkopádné.
- Multi Účelem rozdělovníků je použít jeden příkaz MQPUT k odeslání stejné zprávy do více míst určení. Distribuční seznamy jsou podporovány na systému IBM MQ for Multiplatforms. Distribuční seznamy můžete použít s klastry správců front. V klastru se všechny zprávy rozbalí v MQPUT čase. Výhoda, pokud jde o síťový provoz, není tak velká jako v neklastrovaném prostředí. Výhodou distribučních seznamů je, že četné kanály a přenosové fronty nemusí být definovány ručně.
- Chystáte-li se používat klastry k vyvážení pracovní zátěže, prozkoumejte své aplikace. Zjistěte, zda vyžadují zpracování zpráv konkrétním správcem front nebo v určitém pořadí. O takových žádostech se říká, že mají spřízněnost zpráv. Možná budete muset upravit aplikace, než je budete moci použít ve složitých klastrech.
- Můžete se rozhodnout použít volbu MQOO_BIND_ON_OPEN na MQOPEN , chcete-li vynutit odeslání zpráv do specifického místa určení. Není-li správce cílové fronty k dispozici, nebudou zprávy doručeny, dokud nebude správce front znovu k dispozici. Zprávy nejsou směrovány do jiného správce front kvůli riziku duplikace.
- Má-li být správce front hostitelem úložiště klastru, musíte znát jeho název hostitele nebo adresu IP. Tyto informace musíte zadat do parametru CONNAME při vytváření definice CLUSSDR u jiných správců front, kteří se připojují ke klastru. Používáte-li protokol DHCP, může se IP adresa změnit, protože DHCP může přidělit novou IP adresu pokaždé, když restartujete systém. Proto v definicích CLUSSDR nesmíte uvést adresu IP. I když všechny definice CLUSSDR uvádějí název hostitele spíše než adresu IP, definice by stále nebyly spolehlivé. DHCP nemusí nutně aktualizovat položku adresáře DNS pro hostitele novou adresou. Pokud musíte jmenovat správce front jako úplná úložiště v systémech, které používají protokol DHCP, nainstalujte software, který zaručí, že váš adresář DNS bude aktuální.
- Jako názvy připojení pro kanály nepoužívejte generické názvy, například generické prostředky VTAM nebo generické názvy DDNS (Dynamic Domain Name Server). Pokud tak učiníte, kanály se mohou připojit k jinému správci front, než se očekávalo.
- Zprávu můžete získat pouze z lokální fronty klastru, ale můžete ji vložit do libovolné fronty v klastru. Pokud otevřete frontu pro použití příkazu MQGET , správce front otevře lokální frontu.
- Pokud nastavíte jednoduchý klastr IBM MQ , nemusíte měnit žádnou z aplikací. Aplikace může pojmenovat cílovou frontu ve volání MQOPEN a nemusí vědět o umístění správce front. Pokud nastavíte klastr pro správu pracovní zátěže, musíte zkontrolovat své aplikace a podle potřeby je upravit.
- Aktuální data monitorování a stavu pro kanál nebo frontu můžete zobrazit pomocí příkazů DISPLAY CHSTATUS a DISPLAY QSTATUS **runmqsc** . Informace o monitorování lze použít k měření výkonu a stavu systému. Monitorování je řízeno atributy správce front, fronty a kanálu. Monitorování automaticky definovaných odesílacích kanálů klastru je možné pomocí atributu správce front MONACLS .

Související pojmy

Klastry

“Porovnání klastrování a distribuovaného řazení do front” na stránce 29
Porovnejte komponenty, které je třeba definovat pro připojení správců front pomocí distribuovaného řazení do front a klastrování.

Komponenty klastru

Související úlohy

Konfigurace klastru správců front

Nastavení nového klastru

Jak dlouho uchovávají úložiště správce front informace?

Úložiště správce front uchovávají informace po dobu 30 dnů. Automatický proces efektivně aktualizuje používané informace.

Když správce front odešle některé informace o sobě, správci front úplného a dílčího úložiště tyto informace uloží po dobu 30 dnů. Informace jsou odesílány například v případě, že správce front inzeruje vytvoření nové fronty. Chcete-li zabránit vypršení platnosti těchto informací, správci front po 27 dnech automaticky znovu odešlete všechny informace o sobě. Pokud částečné úložiště odešle novou žádost o informace po dobu životnosti 30 dnů, doba vypršení platnosti zůstane původních 30 dnů.

Po vypršení platnosti informací nedojde k jejich okamžitému odebrání z úložiště. Místo toho se koná po dobu 60 dnů. Není-li během doby odkladu přijata žádná aktualizace, informace se odeberou. Doba odkladu umožňuje skutečnost, že správce front mohl být k datu vypršení platnosti dočasně mimo provoz. Pokud se správce front odpojí od klastru po dobu delší než 90 dnů, přestane být součástí klastru. Pokud se však znovu připojí k síti, stane se součástí klastru znovu. Úplná úložiště nepoužívají informace, jejichž platnost vypršela, k uspokojení nových požadavků od jiných správců front.

Podobně platí, že když správce front odešle požadavek na aktuální informace z úplného úložiště, požadavek trvá 30 dní. Po 27 dnech IBM MQ zkontroluje požadavek. Pokud na něj bylo odkazováno během 27 dnů, bude automaticky aktualizován. Pokud tomu tak není, ponechá se vypršení platnosti a správce front jej v případě potřeby znovu aktualizuje. Vypršení platnosti požadavků zabraňuje hromadění požadavků na informace od neaktivních správců front.

Poznámka: Měli byste stáhnout a nainstalovat opravu PTF pro APAR PH43191, která opraví systémové chyby při výpočtu doby vypršení platnosti odběru. Tyto chyby mohou způsobit předčasné vypršení platnosti odběru (což má za následek vydání zprávy CSQX456I) nebo vypršení platnosti po vypršení platnosti objektu (což má za následek chyby MQRC 2085 (MQRC_UNKNOWN_OBJECT)).

V případě velkých klastrů může být s přerušením, pokud mnoho správců front automaticky znovu připojí všechny informace o sobě současně. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.

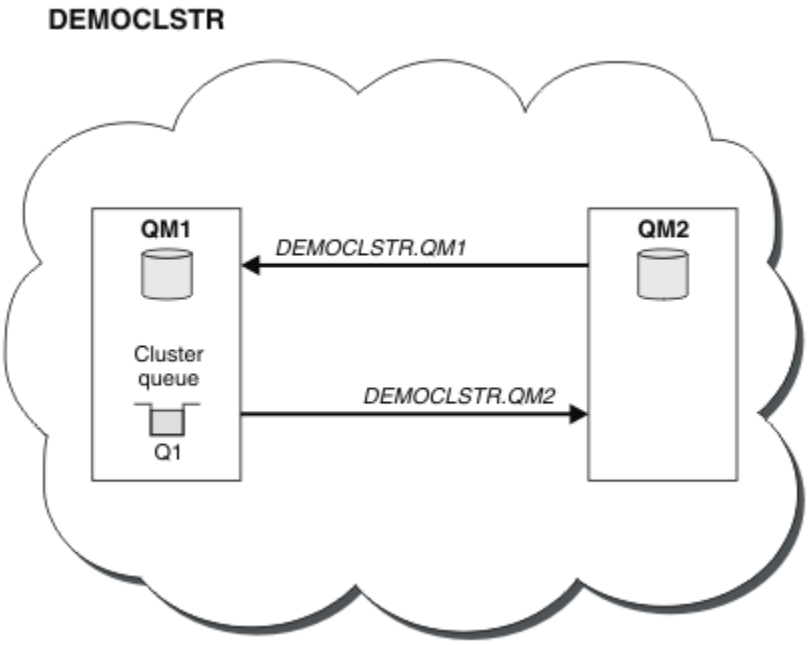
Související pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 66
Pomocí příkazu **REFRESH CLUSTER** vyřadíte všechny lokálně uchovávané informace o klastru a znovu sestavíte tyto informace z úplných úložišť v klastru. Tento příkaz byste neměli používat, s výjimkou výjimečných okolností. Pokud jej potřebujete použít, existují speciální pokyny pro jeho použití. Tyto informace jsou vodítkem na základě testování a zpětné vazby od zákazníků.

Vzorové klastry

První příklad zobrazuje nejmenší možný klastr dvou správců front. Druhý a třetí příklad ukazují dvě verze tří klastrů správců front.

Nejmenší možný klastr obsahuje pouze dva správce front. V tomto případě obsahují oba správci front úplná úložiště. Chcete-li nastavit klastr, potřebujete pouze několik definic, a přesto je v každém správci front vysoký stupeň autonomie.



Obrázek 8. Malý klastr se dvěma správci front

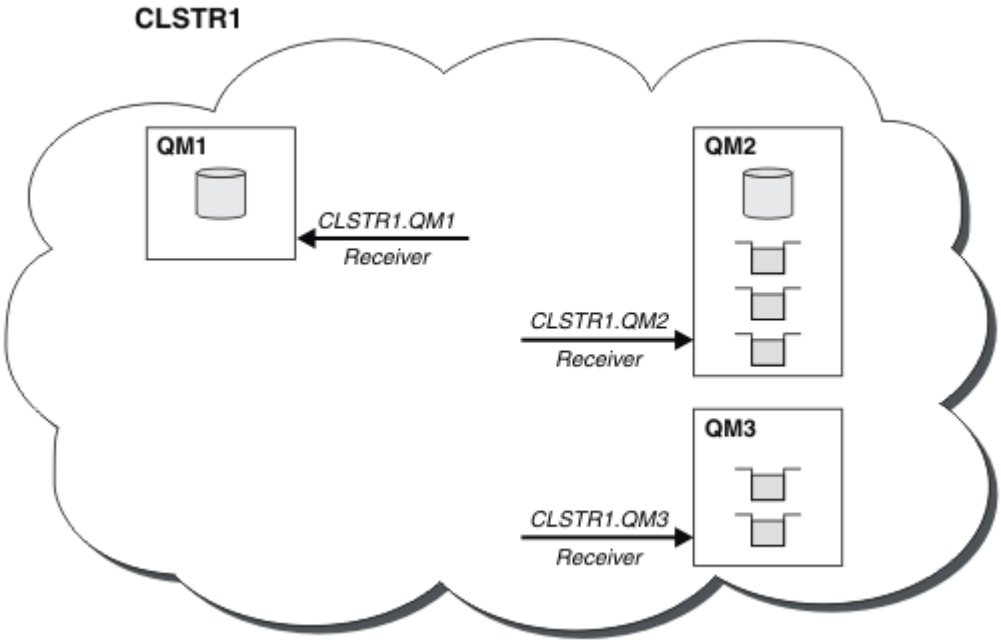
- Správci front mohou mít dlouhé názvy, například LONDON a NEWYORK. z/OS V systému IBM MQ for z/OSjsou názvy správců front omezeny na čtyři znaky.
- Každý správce front je obvykle konfigurován na samostatném počítači. V jednom počítači však může být více správců front.

Pokyny k nastavení podobného ukázkového klastru naleznete v tématu Nastavení nového klastru.

Obrázek 9 na stránce 39 zobrazuje komponenty klastru s názvem CLSTR1.

- V tomto klastru jsou tři správci front, QM1, QM2a QM3.
- QM1 a QM2 hostují úložiště informací o všech správcích front a objektech souvisejících s klastrem v klastru. Nazývají se *správci front úplného úložiště*. Úložiště jsou v diagramu reprezentována stínovaným cylindrem.
- QM2 a QM3 hostují některé fronty, které jsou přístupné pro všechny ostatní správce front v klastru. Fronty, které jsou přístupné pro všechny ostatní správce front v klastru, se nazývají *fronty klastru*. Fronty klastru jsou v diagramu reprezentovány stínovými frontami. Fronty klastru jsou přístupné odkudkoli v klastru. Kód klastrování produktu IBM MQ zajišťuje, že definice vzdálených front pro fronty klastru jsou vytvářeny ve všech správcích front, kteří na ně odkazují.

  Stejně jako v případě distribuovaného řazení do front používá aplikace volání MQPUT k vložení zprávy do fronty klastru v libovolném správci front v klastru. Aplikace používá volání MQGET k načtení zpráv z fronty klastru pouze ve správci front, kde je fronta umístěna.
- Každý správce front má ručně vytvořenou definici pro přijímací konec kanálu s názvem *cluster_name*. *queue_manager_name* , v němž může přijímat zprávy. V přijímajícím správci front je *cluster_name*. *queue_manager_name* přijímacím kanálem klastru. Přijímací kanál klastru je jako přijímací kanál používaný v distribuovaných frontách; přijímá zprávy pro správce front. Kromě toho také obdrží informace o klastru.

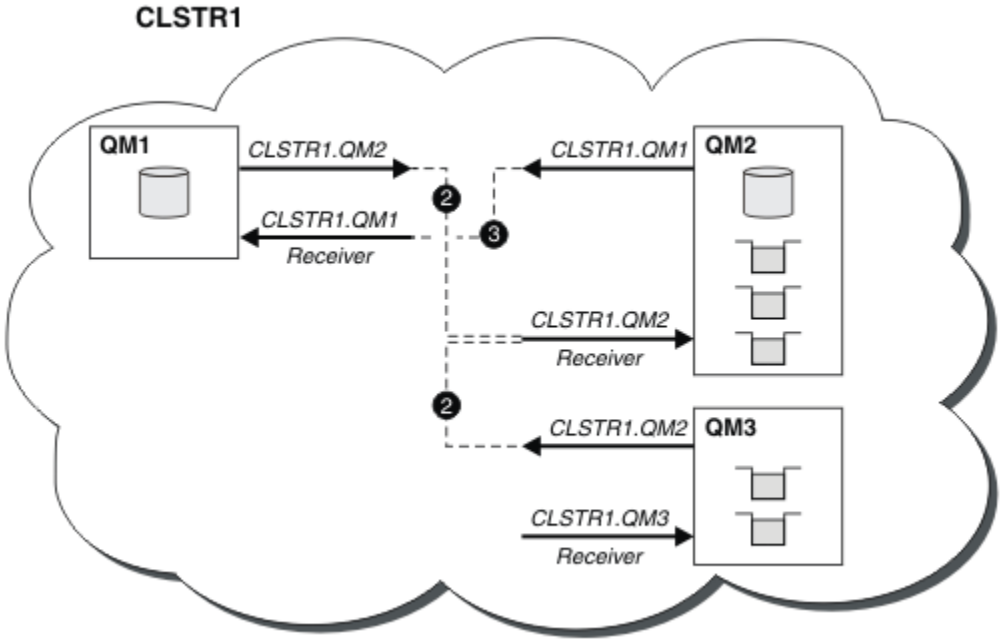


Obrázek 9. Klastr správců front

- V produktu Obrázek 10 na stránce 39 má každý správce front také definici pro odesílající konec kanálu. Připojuje se ke kanálu příjemce klastru jednoho ze správců front úplného úložiště. V odesílajícím správci front je *cluster_name. queue_manager_name* odesílacím kanálem klastru. QM1 a QM3 mají odesílací kanály klastru, které se připojují k CLSTR1.QM2, viz tečkovaná čára "2".

  QM2 má kanál odesilatele klastru připojující se k CLSTR1.QM1, viz tečkovaná čára "3". Odesílací kanál klastru je jako odesílací kanál používaný při distribuovaném řazení do front. Odesílá zprávy přijímajícímu správci front. Kromě toho také odesílá informace o klastru.

  Jakmile je definován konec příjemce klastru i konec odesílatele klastru kanálu, kanál se spustí automaticky.

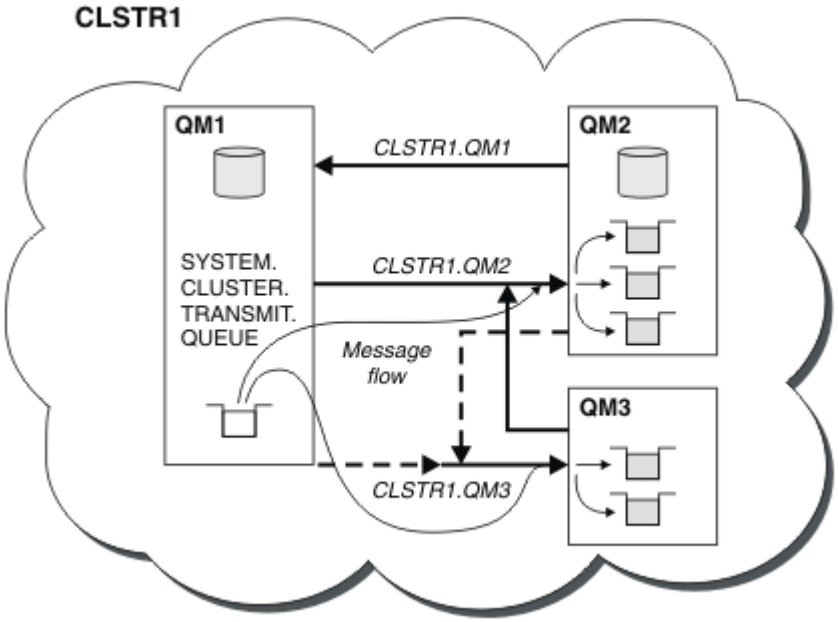


Obrázek 10. Klastr správců front s odesílacími kanály

Definování odesílacího kanálu klastru v lokálním správci front zavede tohoto správce front do jednoho ze správců front úplného úložiště. Správce front úplného úložiště příslušným způsobem aktualizuje informace ve svém úplném úložišti. Poté automaticky vytvoří odesílací kanál klastru zpět do původního správce front a odešle informace o tomto správci front o klastru. Proto se správce front dozví o klastru a klastr o správci front.

Podívejte se znovu na Obrázek 9 na stránce 39. Předpokládejme, že aplikace připojená ke správci front QM3 chce odeslat některé zprávy do front v adresáři QM2. Při prvním přístupu k těmto frontám musí produkt QM3 tyto fronty zjistit prostřednictvím konzultace s úplným úložištěm. Úplné úložiště v tomto případě je QM2, ke kterému se přistupuje pomocí kanálu odesilatele CLSTR1.QM2. Pomocí informací z úložiště může automaticky vytvářet vzdálené definice pro tyto fronty. Pokud jsou fronty v systému QM1, tento mechanizmus stále funguje, protože QM2 je úplné úložiště. Úplné úložiště obsahuje úplný záznam všech objektů v klastru. V tomto druhém případě produkt QM3 také automaticky vytvoří odesílací kanál klastru odpovídající přijímacímu kanálu klastru v systému QM1, což umožní přímou komunikaci mezi těmito dvěma kanály.

Obrázek 11 na stránce 40 zobrazuje stejný klastr se dvěma odesílacími kanály klastru, které byly vytvořeny automaticky. Odesílací kanály klastru jsou reprezentovány dvěma přerušovanými čarami, které se spojují s přijímacím kanálem klastru CLSTR1.QM3. Také zobrazuje přenosovou frontu klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE, kterou produkt QM1 používá k odesílání svých zpráv. Všichni správci front v klastru mají přenosovou frontu klastru, ze které mohou odesílat zprávy všem ostatním správcům front ve stejném klastru.



Obrázek 11. Klastr správců front zobrazující automaticky definované kanály.

Poznámka: Ostatní diagramy zobrazují pouze přijímající konce kanálů, pro které provedete ruční definice. Odesílající konce jsou vynechány, protože jsou většinou definovány automaticky v případě potřeby. Automatická definice většiny odesílacích kanálů klastru je zásadní pro funkci a efektivitu klastrů.

Související pojmy

“Porovnání klastrování a distribuovaného řazení do front” na stránce 29
Porovnejte komponenty, které je třeba definovat pro připojení správců front pomocí distribuovaného řazení do front a klastrování.

Komponenty klastru

Související úlohy

Konfigurace klastru správců front

Nastavení nového klastru

Klastrování: Nejlepší postupy

Klastry poskytují mechanizmus pro propojování správců front. Doporučené postupy popsané v této části jsou založeny na testování a zpětné vazbě od zákazníků.

Úspěšné nastavení klastru závisí na dobrém plánování a důkladném pochopení principů IBM MQ , jako je například dobrá správa aplikací a návrh sítě. Než budete pokračovat, ujistěte se, že jste obeznámeni s informacemi v souvisejících tématech.

Související pojmy

Distribuované řazení do front a klastry

Klastry

Související úlohy

“Návrh klastrů” na stránce 22

Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Klastry musí být pečlivě navrženy tak, aby zajistily, že budou správně fungovat a že dosáhnou požadované úrovně dostupnosti a schopnosti reagovat.

Monitorování klastrů

Klastrování: Zvláštní aspekty pro překrývající se klastry

Toto téma poskytuje pokyny pro plánování a administraci klastrů IBM MQ . Tyto informace jsou vodítkem na základě testování a zpětné vazby od zákazníků.

Vlastnictví klastru

Před čtením následujících informací se seznamte s překrývajícími se klastry. Potřebné informace viz “Překrývající se klastry” na stránce 34 a Konfigurace cest zpráv mezi klastry .

Při konfiguraci a správě systému, který se skládá z překrývajících se klastrů, je nejlepší dodržovat následující:

- Ačkoli jsou klastry IBM MQ 'volně spřaženy', jak bylo popsáno výše, je vhodné považovat klastr za jednu jednotku administrace. Tento koncept se používá, protože interakce mezi definicemi v jednotlivých správcích front je kritická pro hladké fungování klastru. Například: Při použití front klastru s vyrovnanou pracovní zátěží je důležité, aby jeden administrátor nebo tým porozuměli úplné sadě možných cílů pro zprávy, které závisí na definicích rozmístěných v rámci klastru. Více triviálně, dvojice odesílací/přijímací kanál klastru musí být kompatibilní v celém.
- Vzhledem k tomuto předchozímu konceptu, kdy se setkávají vícenásobné klastry (které mají být spravovány samostatnými týmy/jednotlivci), je důležité mít jasné zásady pro řízení administrace správců front brány.
- Je užitečné považovat překrývající se klastry za jeden obor názvů: názvy kanálů a názvy správců front musí být jedinečné v rámci jednoho klastru. Administrace je mnohem jednodušší, když je jedinečná v celé topologii. Nejlepší je postupovat podle vhodné konvence pojmenování, možné konvence jsou popsány v části “Konvence pojmenování klastrů” na stránce 33.
- Někdy je nezbytná spolupráce v oblasti správy a řízení systému. Například spolupráce mezi organizacemi, které vlastní různé klastry, které se musí překrývat. Jasné pochopení toho, kdo co vlastní, a vymahatelná pravidla a konvence pomáhají klastrování fungovat hladce při překrývajících se klastrech.

Překrývající se klastry: Brány

Obecně platí, že spravovat jeden klastr je jednodušší než spravovat více klastrů. Proto je třeba se obecně vyhnout vytváření velkého počtu malých klastrů (například pro každou aplikaci).

Chcete-li však poskytovat provozní třídy, můžete implementovat překrývající se klastry. Příklad:

- Pokud máte soustředné klastry, kde menší je pro publikování/odběr. Další informace viz Jak velikostovat systémy .

- Pokud mají být někteří správci front spravováni různými týmy. Další informace naleznete v předchozí části “Vlastnictví klastru” na stránce 41.
- Pokud to dává smysl z organizačního nebo geografického hlediska.
- Pokud ekvivalentní klastry pracují s rozpoznáním názvů, například při implementaci TLS v existujícím klastru.

Překrývající se klastry nepřinášejí žádný přínos pro zabezpečení; umožňují překrývání klastrů spravovaných dvěma různými týmy a efektivně se připojují k týmům i k topologii:

- Jakýkoli název inzerovaný v takovém klastru je přístupný pro jiný klastr.
- Jakýkoli název inzerovaný v jednom klastru může být inzerován v druhém klastru, aby se odčerpaly vhodné zprávy.
- Jakýkoli neinzerovaný objekt ve správci front, který sousedí s bránou, lze interpretovat z libovolného klastru, jehož je brána členem.

Obor názvů je sjednocením obou klastrů a musí být považován za jeden obor názvů. Proto je vlastnictví překrývajících se klastrů sdíleno mezi všemi administrátory obou klastrů.

Pokud systém obsahuje více klastrů, může být nutné směrovat zprávy ze správců front v jednom klastru do front ve správcích front v jiném klastru. V této situaci musí být více klastrů nějakým způsobem propojeno: Dobrý vzor, který je třeba dodržet, je použití správců front brány mezi klastry. Toto uspořádání se vyhýbá vytváření sítě kanálů typu point-to-point, která je obtížně spravovatelné, a poskytuje vhodné místo pro správu takových otázek, jako jsou bezpečnostní politiky. Existují dva různé způsoby, jak dosáhnout tohoto uspořádání:

1. Umístěte jednoho (nebo více) správců front do obou klastrů pomocí druhé definice příjemce klastru. Toto uspořádání zahrnuje méně administrativních definic, ale jak již bylo uvedeno, znamená, že vlastnictví překrývajících se klastrů je sdíleno všemi administrátory obou klastrů.
2. Spárujte správce front v klastru jedna se správcem front v klastru dva pomocí tradičních kanálů dvoubodového spojení.

V každém z těchto případů lze pro správné směrování provozu použít různé nástroje. Pro směrování do jiného klastru lze použít zejména aliasy front nebo správců front a alias správce front s prázdnou vlastností **RQMNAME** znovu vyvažuje pracovní zátěž tam, kde je to žádoucí.

Související pojmy

“Konvence pojmenování klastrů” na stránce 33
Zvažte pojmenování správců front ve stejném klastru pomocí konvence pojmenování, která identifikuje klastr, do kterého správce front patří. Použijte podobnou konvenci pojmenování pro názvy kanálů a rozšiřte ji tak, aby popisovala charakteristiku kanálu.

Klastrování: Pokyny pro návrh topologie

Toto téma poskytuje pokyny pro plánování a administraci klastrů IBM MQ . Tyto informace jsou vodítkem na základě testování a zpětné vazby od zákazníků.

Přemýšlíte-li o tom, kde budou předem umístěny uživatelské aplikace a interní administrativní procesy, můžete se vyhnout mnoha problémům nebo je později minimalizovat. Toto téma obsahuje informace o návrhových rozhodnutích, která mohou zlepšit výkon a zjednodušit úlohy údržby při rozšiřování klastru.

- “Výkon klastrovací infrastruktury” na stránce 42
- “Úplná úložiště” na stránce 43
- “Mají aplikace používat fronty v úplných úložištích?” na stránce 44
- “Správa definic kanálů” na stránce 44
- “Vyrovnávání pracovní zátěže prostřednictvím více kanálů” na stránce 45

Výkon klastrovací infrastruktury

Když se aplikace pokusí otevřít frontu ve správci front v klastru, zaregistruje svůj zájem s úplnými úložišti pro tuto frontu, aby se mohla dozvědět, kde fronta v klastru existuje. Veškeré aktualizace umístění nebo

konfigurace fronty jsou automaticky odesílány úplnými úložišti do zainteresovaných správců front. Tato registrace, která je předmětem zájmu, je interně označována jako odběr (tyto odběry nejsou stejné jako odběry produktu IBM MQ používané pro systém zpráv publikování/odběru v produktu IBM MQ).

Veškeré informace o klastru procházejí každým úplným úložištěm. Úplná úložiště se proto vždy používají v klastru pro administrativní přenos zpráv. Vysoké využití systémových prostředků při správě těchto odběrů a jejich přenos a výsledné konfigurační zprávy mohou způsobit značné zatížení infrastruktury klastrování. Existuje řada věcí, které je třeba zvážit při zajištění toho, aby bylo toto zatížení chápáno a minimalizováno, kdykoli je to možné:

- Čím více jednotlivých správců front používajících frontu klastru, tím více odběrů je v systému, a tím větší administrativní režie v případě změn a zainteresovaných odběratelů je třeba upozornit, zejména na správce front úplného úložiště. Jedním ze způsobů, jak minimalizovat zbytečný provoz a úplné zatížení úložiště, je připojení podobných aplikací (tj. aplikací, které pracují se stejnými frontami) k menšímu počtu správců front.
- Kromě počtu odběrů v systému, které ovlivňují výkon, může četnost změn v konfiguraci klastrovaných objektů ovlivnit výkon, například častou změnu konfigurace klastrované fronty.
- Je-li správce front členem více klastrů (tj. je součástí překrývajících se klastrových systémů), výsledkem jakéhokoli zájmu o frontu je odběr pro každý klastr, jehož je členem, a to i v případě, že stejní správci front jsou úplnými úložišti pro více klastrů. Toto uspořádání zvyšuje zátěž systému a je jedním z důvodů, proč zvážit, zda je zapotřebí více překrývajících se klastrů, spíše než jeden klastr.
- Přenos zpráv aplikace (tj. zpráv odesílaných aplikacemi IBM MQ do front klastru) neprobíhá prostřednictvím úplných úložišť a nedosahuje ke správcům cílových front. Tento přenos zpráv je odesílán přímo mezi správcem front, ve kterém zpráva vstupuje do klastru, a správcem front, ve kterém fronta klastru existuje. Proto není nutné pojmout vysoký počet přenosů zpráv aplikace s ohledem na správce front úplného úložiště, pokud není správce front úplného úložiště jedním z uvedených dvou správců front. Z tohoto důvodu se doporučuje, aby správci front úplného úložiště nebyli používáni pro provoz zpráv aplikace v klastrech, kde je zátěž infrastruktury klastrování významná.

Úplná úložiště

Úložiště je kolekce informací o správcích front, kteří jsou členy klastru. Správce front, který je hostitelem úplné sady informací o každém správci front v klastru, má úplné úložiště. Další informace o úplných úložištích a dílčích úložištích naleznete v tématu Klastrové úložiště.

Úplná úložiště musí být uchovávána na serverech, které jsou spolehlivé a co nejvíce dostupné, a je třeba se vyhnout jednotlivým bodům selhání. Návrh klastru musí mít vždy dvě úplná úložiště. Dojde-li k selhání úplného úložiště, může klastr i nadále fungovat.

Podrobnosti o všech aktualizacích prostředků klastru provedených správcem front v klastru; například klastrované fronty jsou odesílány z tohoto správce front nejvýše do dvou úplných úložišť v daném klastru (nebo do jednoho, pokud v klastru existuje pouze jeden správce front úplného úložiště). Tato úplná úložiště uchovávají informace a rozšiřují je na všechny správce front v klastru, kteří o ně projeví zájem (tj. odebírají se k nim). Chcete-li zajistit, aby každý člen klastru měl aktuální pohled na prostředky klastru, musí být každý správce front schopen komunikovat s alespoň jedním správcem front úplného úložiště současně.

Pokud z nějakého důvodu nemůže správce front komunikovat s žádnými úplnými úložišti, může i nadále fungovat v klastru na základě úrovně informací, které jsou již uloženy v mezipaměti, ale nejsou k dispozici žádné nové aktualizace nebo přístup k dříve nepoužitým prostředkům klastru.

Z tohoto důvodu musíte usilovat o to, aby byla vždy k dispozici dvě úplná úložiště. Toto uspořádání však neznamená, že musí být přijata extrémní opatření, protože klastr funguje dostatečně krátkou dobu bez úplného úložiště.

Existuje další důvod, proč klastr musí mít dva správce front úplného úložiště, kromě dostupnosti informací o klastru: Důvodem je zajistit, aby informace o klastru uložené v mezipaměti úplného úložiště existovaly pro účely zotavení na dvou místech. Pokud existuje pouze jedno úplné úložiště a ztratí informace o klastru, je vyžadován ruční zásah do všech správců front v klastru, aby klastr znovu fungoval. Pokud však existují

dvě úplná úložiště, pak vzhledem k tomu, že informace jsou vždy publikovány a přihlášeny k odběru ze dvou úplných úložišť, lze nezdařené úplné úložiště obnovit s minimálním úsilím.

- Je možné provádět údržbu správců front s úplným úložištěm ve dvou návrhových klastrech s úplným úložištěm bez dopadu na uživatele tohoto klastru: Klastr nadále pracuje pouze s jedním úložištěm, takže pokud je to možné, vypněte úložiště, proveďte údržbu a proveďte zálohu znovu po jednom. I když dojde k výpadku na druhém úplném úložišti, spuštěné aplikace nejsou ovlivněny po dobu nejméně tří dnů.
- Pokud neexistuje dobrý důvod pro použití třetího úložiště, například pro použití geograficky lokálního úplného úložiště z geografických důvodů, použijte návrh dvou úložišť. Použití tří úplných úložišť znamená, že nikdy nevíte, které dvě z nich se právě používají, a může dojít k administrativním problémům způsobeným interakcemi mezi více parametry správy pracovní zátěže. Nedoporučuje se mít více než dvě úplná úložiště.
- Pokud stále potřebujete lepší dostupnost, zvažte hostování správců front úplného úložiště jako správců front s více instancemi nebo použití podpory vysoké dostupnosti specifické pro platformu ke zlepšení jejich dostupnosti.
- Je třeba plně propojit všechny správce front úplného úložiště s ručně definovanými odesílacími kanály klastru. Zvláštní pozornost je třeba věnovat situaci, kdy klastr má z nějakého oprávněného důvodu více než dvě úplná úložiště. V této situaci je často možné vynechat jeden nebo více kanálů a aby to nebylo okamžitě zřejmé. Když nedojde k úplnému propojení, problémy se často diagnostikují. Je těžké je diagnostikovat, protože některá úplná úložiště neuchovávají všechna data úložiště, a proto mají správci front v klastru různá zobrazení klastru v závislosti na úplných úložištích, ke kterým se připojují.

Mají aplikace používat fronty v úplných úložištích?

Úplné úložiště je ve většině případů stejné jako kterýkoli jiný správce front, a proto je možné hostovat fronty aplikací v úplném úložišti a připojovat aplikace přímo k těmto správcům front. Mají aplikace používat fronty v úplných úložištích?

Běžně přijímaná odpověď je "Ne?". Ačkoli je tato konfigurace možná, mnoho zákazníků raději ponechá tyto správce front vyhrazené pro údržbu mezipaměti klastru úplného úložiště. Zde jsou popsány body, které je třeba zvážit při rozhodování o jedné z možností, ale nakonec musí být architektura klastru vhodná pro konkrétní požadavky prostředí.

- Upgrady: Aby bylo možné používat nové funkce klastru v nových verzích produktu IBM MQ , musí být nejprve upgradováni správci front úplného úložiště daného klastru. Pokud chce aplikace v klastru používat nové funkce, může být užitečné aktualizovat úplná úložiště (a některá dílčí úložiště) bez testování řady společně umístěných aplikací.
- Údržba: Podobně, pokud musíte použít naléhavou údržbu na úplná úložiště, lze je restartovat nebo obnovit pomocí příkazu **REFRESH** , aniž byste se dotkli aplikací.
- Výkon: Vzhledem k tomu, že se klastry rozšiřují a požadavky na údržbu mezipaměti klastru s úplným úložištěm se zvyšují, oddělená správa aplikací snižuje riziko ovlivnění výkonu aplikací prostřednictvím soupeření o systémové prostředky.
- Hardwarové požadavky: Úplná úložiště obvykle nemusí být výkonná; stačí například jednoduchý server UNIX s dobrým očekáváním dostupnosti. Alternativně pro velmi velké nebo neustále se měnící klastry je třeba zvážit výkon počítače s úplným úložištěm.
- Požadavky na software: Požadavky jsou obvykle hlavním důvodem pro výběr hostitele front aplikací v úplném úložišti. V malém klastru může kolokace znamenat požadavek na méně správců front/serverů nad všemi.

Správa definic kanálů

I v rámci jednoho klastru může existovat více definic kanálů, které poskytují více tras mezi dvěma správci front.

Někdy je výhodou mít paralelní kanály v rámci jednoho klastru, ale toto rozhodnutí o návrhu musí být důkladně zváženo; kromě toho, že přidáte složitost, může tento návrh vést k nedostatečně používaným kanálům, což snižuje výkon. K této situaci dochází, protože testování obvykle zahrnuje odesílání velkého

množství zpráv konstantní rychlostí, takže paralelní kanály jsou plně využívány. Při reálných podmínkách nekonstantního proudu zpráv však algoritmus vyrovnávání pracovní zátěže způsobí pokles výkonu při přepnutí toku zpráv z kanálu na kanál.

Je-li správce front členem více klastrů, existuje volba pro použití definice jednoho kanálu se seznamy názvů klastrů, nikoli pro definování samostatného kanálu CLUSRCVR pro každý klastr. Toto nastavení však může později způsobit potíže s administrací; zvažte například případ, kdy se má TLS použít na jeden klastr, ale ne na druhý. Proto je vhodnější vytvořit samostatné definice a tuto možnost podporuje konvence pojmenování navržené v produktu “Konvence pojmenování klastrů” na stránce 33 .

Vyrovnávání pracovní zátěže prostřednictvím více kanálů

Tyto informace jsou určeny jako rozšířená znalost předmětu. Základní vysvětlení tohoto předmětu (kterému je třeba porozumět před použitím těchto informací) naleznete v tématu Použití klastrů pro správu pracovní zátěže, Vyvažování pracovní zátěže v klastrecha Algoritmus správy pracovní zátěže klastru.

Algoritmus správy pracovní zátěže klastru poskytuje velkou sadu nástrojů, ale nesmí být všechny používány navzájem, aniž by plně porozuměli tomu, jak pracují a interaktivně spolupracují. Je možné, že není zřejmé, jak důležité kanály jsou pro proces vyrovnávání pracovní zátěže: Algoritmus round-robin správy pracovní zátěže se chová, jako by se více kanálů klastru pro správce front, který vlastní klastrovanou frontu, považovalo za více instancí této fronty. Tento proces je podrobněji vysvětlen v následujícím příkladu:

1. V klastru jsou dva správci front, kteří jsou hostiteli fronty: QM1 a QM2.
2. Do adresáře QM1je pět přijímacích kanálů klastru.
3. Do adresáře QM2existuje pouze jeden přijímací kanál klastru.
4. Když **MQPUT** nebo **MQOPEN** na QM3 zvolí instanci, algoritmus je pětkrát pravděpodobnější, že odešle zprávu do QM1 než do QM2.
5. Situace v kroku 4 se vyskytne, protože algoritmus vidí šest voleb, ze kterých si můžete vybrat (5 + 1) a round-robins ve všech pěti kanálech do QM1 a jeden kanál do QM2.

Dalším nepatrným chováním je, že i při vkládání zpráv do klastrované fronty, která má v lokálním správci front nakonfigurovanou jednu instanci, produkt IBM MQ použije stav kanálu příjemce lokálního klastru k rozhodnutí, zda mají být zprávy vkládány do lokální instance fronty nebo vzdálených instancí fronty. V tomto scénáři:

1. Při vkládání zpráv algoritmus správy pracovní zátěže nezkoumá jednotlivé fronty klastru, ale kanály klastru, které mohou dosáhnout těchto cílů.
2. Pro dosažení lokálních cílů jsou v tomto seznamu zahrnuty lokální přijímací kanály (i když nejsou použity k odeslání zprávy).
3. Je-li lokální přijímací kanál zastaven, algoritmus správy pracovní zátěže standardně preferuje alternativní instanci, není-li jeho CLUSRCVR zastaven. Pokud existuje více lokálních instancí CLUSRCVR pro místo určení a alespoň jedna není zastavena, lokální instance zůstává způsobilá.

Klastrování: Izolace aplikace pomocí více přenosových front klastru
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášené různými odesílacími kanály klastru můžete umístit do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma poskytuje příklady a některé doporučené postupy, které vás provedou výběrem přístupu k použití.

Při implementaci aplikace máte na výběr, které prostředky produktu IBM MQ sdílí s jinými aplikacemi a které prostředky nesdílí. Existuje řada typů prostředků, které lze sdílet, přičemž hlavní z nich je samotný server, správce front, kanály a fronty. Můžete se rozhodnout konfigurovat aplikace s menším počtem sdílených prostředků; přidělovat jednotlivým aplikacím samostatné fronty, kanály, správce front nebo dokonce servery. Pokud tak učiníte, celková konfigurace systému se stane větší a složitější. Použití klastrů IBM MQ snižuje složitost správy více serverů, správců front, front a kanálů, ale zavádí další sdílený prostředek, přenosovou frontu klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Obrázek 12 na stránce 47 je výseč z velké implementace produktu IBM MQ , která ilustruje význam sdílení SYSTEM.CLUSTER.TRANSMIT.QUEUE. V diagramu je aplikace Client Apppřipojena ke správci front QM2 v klastru CL1. Zpráva z produktu Client App je zpracována aplikací Server App. Zprávu načte produkt Server App z fronty klastru Q1 ve správci front QM3 v souboru CLUSTER2. Vzhledem k tomu, že aplikace klienta a serveru nejsou ve stejném klastru, je zpráva přenesena správcem front brány QM1.

Běžným způsobem konfigurace brány klastru je nastavit správce front brány jako člena všech klastrů. Ve správci front brány jsou definovány klastrované alias fronty pro fronty klastru ve všech klastrech. Aliasy klastrované fronty jsou k dispozici ve všech klastrech. Zprávy vkládané do aliasů fronty klastru jsou směrovány prostřednictvím správce front brány do správného místa určení. Správce front brány vkládá zprávy odeslané do klastrovaných alias front do společného SYSTEM.CLUSTER.TRANSMIT.QUEUE v systému QM1.

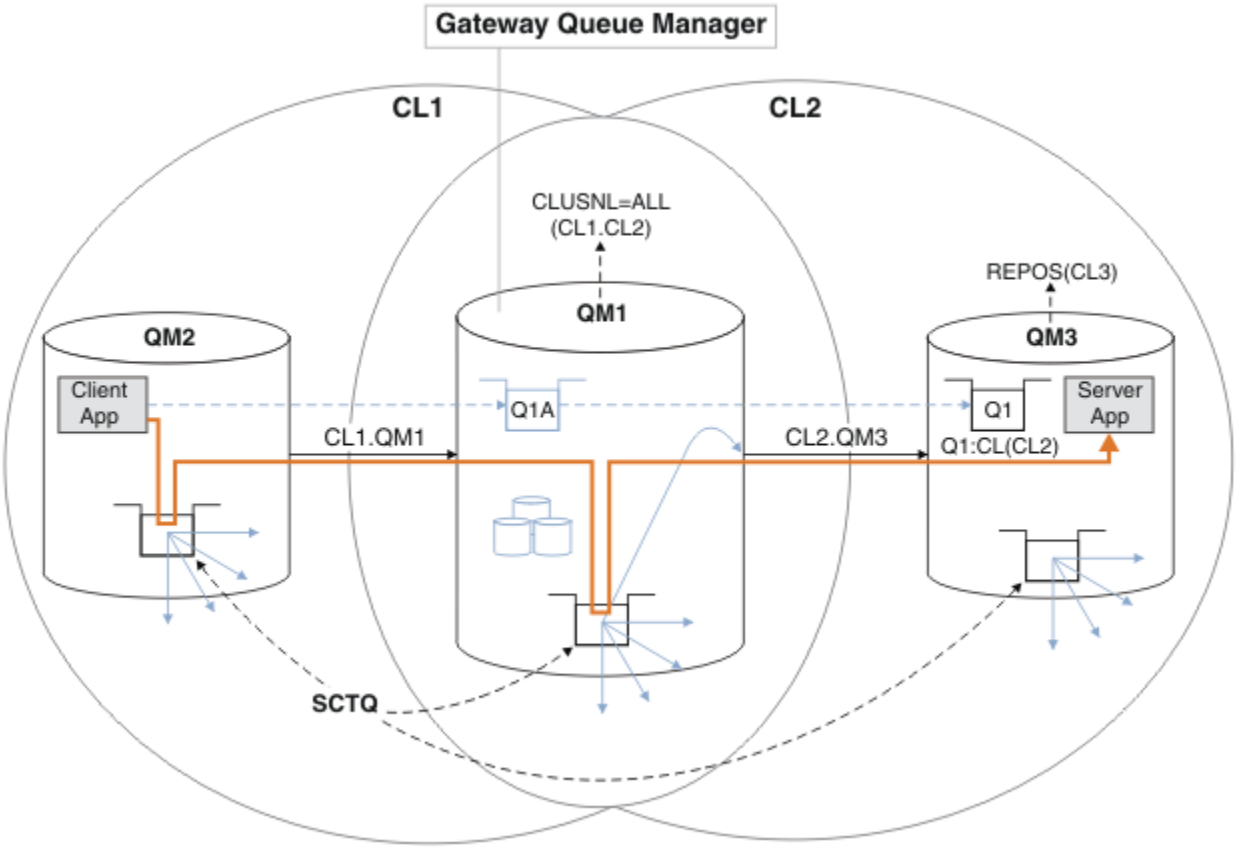
Centrální a paprsková architektura vyžaduje, aby všechny zprávy mezi klastry prošly přes správce front brány. Výsledkem je, že všechny zprávy procházejí přenosovou frontou jednoho klastru v systému QM1, SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Z hlediska výkonu se nejedná o problém s jedinou frontou. Společná přenosová fronta obecně nepředstavuje kritické místo výkonu. Propustnost zpráv na bráně je do značné míry určena výkonem kanálů, které se k ní připojují. Propustnost není obecně ovlivněna počtem front nebo počtem zpráv ve frontách, které kanály používají.

Z některých dalších perspektiv má použití jedné přenosové fronty pro více aplikací nevýhody:

- Tok zpráv do jednoho místa určení nelze izolovat od toku zpráv do jiného místa určení. Úložiště zpráv před jejich předáním nelze oddělit, a to ani v případě, že se místa určení nacházejí v různých klastrech v různých správcích front.

  Pokud se jedno místo určení klastru stane nedostupným, zprávy pro toto místo určení se sestaví v jedné přenosové frontě a nakonec se zprávy naplní. Jakmile je přenosová fronta plná, zastaví umisťování zpráv do přenosové fronty pro libovolné místo určení klastru.
- Není snadné monitorovat přenos zpráv do různých cílů klastru. Všechny zprávy jsou v jedné přenosové frontě. Zobrazení hloubky přenosové fronty vám poskytuje málo informací o tom, zda jsou zprávy přenášeny do všech cílů.



Poznámka: Šipky v souboru Obrázek 12 na stránce 47 a následující obrázky mají různé typy. Plné šipky představují toky zpráv. Popisky na plných šipkách jsou názvy kanálů zpráv. Šedé plné šipky jsou potenciální toky zpráv z produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE do odesílacích kanálů klastru. Černé přerušované čáry spojují popisky s cíli. Šedé čárkované šipky jsou odkazy; například z MQOPEN volání `Client` App do definice fronty aliasu klastru Q1A.

Obrázek 12. Aplikace klient-server implementovaná na centrální a paprskovou architekturu pomocí klastrů IBM MQ

V systému Obrázek 12 na stránce 47klienti `Server` App otevřou frontu Q1A. Zprávy jsou vloženy do systému SYSTEM.CLUSTER.TRANSMIT.QUEUE v systému QM2, přeneseny do systému SYSTEM.CLUSTER.TRANSMIT.QUEUE v systému QM1a poté přeneseny do systému Q1 v systému QM3, kde jsou přijímány aplikací `Server` App .

Zpráva z produktu `Client` App prochází systémovými přenosovými frontami klastru v systémech QM2 a QM1. V produktu Obrázek 12 na stránce 47je cílem izolovat tok zpráv ve správci front brány od klientské aplikace, aby jeho zprávy nebyly uloženy v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE. Můžete izolovat toky na všech ostatních klastrovaných správcích front. Můžete také izolovat toky v opačném směru, zpět ke klientovi. Chcete-li stručně popsat popisy řešení, zvažte pouze jeden tok z klientské aplikace.

Řešení pro izolaci provozu zpráv klastru ve správci front brány klastru

Jedním ze způsobů, jak problém vyřešit, je použít aliasy správce front nebo definice vzdálených front k přemostění mezi klastry. Vytvořte definici klastrované vzdálené fronty, přenosovou frontu a kanál, abyste oddělili jednotlivé toky zpráv ve správci front brány. Viz téma Přidání definice vzdálené fronty pro izolování zpráv odeslaných ze správce front brány.

Počínaje produktem IBM WebSphere MQ 7.5 nejsou správci front klastru omezeni na jednu přenosovou frontu klastru. Můžete vybrat ze dvou voleb:

1. Ručně definujte další přenosové fronty klastru a definujte, které odesílací kanály klastru přenášejí zprávy z jednotlivých přenosových front. Viz téma Přidání přenosové fronty klastru k izolaci přenosu zpráv klastru odeslaných ze správce front brány.
2. Povolit správci front automatické vytváření a správu dalších přenosových front klastru. Definuje jinou přenosovou frontu klastru pro každý odesílací kanál klastru; viz Změna výchozího nastavení na oddělené přenosové fronty klastru pro izolaci přenosu zpráv.

Můžete kombinovat ručně definované přenosové fronty klastru pro některé odesílací kanály klastru se správcem front spravujícím zbytek. Kombinace přenosových front je metodou, která je použita v tématu Přidání přenosové fronty klastru k izolaci provozu zpráv klastru odeslaných ze správce front brány. V tomto řešení většina zpráv mezi klastry používá společný soubor `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Jedna aplikace je kritická a všechny její toky zpráv jsou izolovány od ostatních toků pomocí jedné ručně definované přenosové fronty klastru.

Konfigurace v části Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány je omezena. Neodděluje přenos zpráv do fronty klastru ve stejném správci front ve stejném klastru jako jiná fronta klastru. Přenos zpráv do jednotlivých front můžete oddělit pomocí definic vzdálených front, které jsou součástí distribuovaných front. U klastrů můžete pomocí více přenosových front klastru oddělit přenos zpráv, který se používá pro různé odesílací kanály klastru. Více front klastru ve stejném klastru ve stejném správci front sdílí odesílací kanál klastru. Zprávy pro tyto fronty jsou před předáním ze správce front brány uloženy ve stejné přenosové frontě. V konfiguraci v části Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaného ze správce front brányje omezení vystupňováno přidáním dalšího klastru a nastavením správce front a fronty klastru jako člena nového klastru. Nový správce front může být jediným správcem front v klastru. Do klastru můžete přidat další správce front a použít stejný klastr k izolaci front klastru i v těchto správcích front.

Související pojmy

“Řízení přístupu a více přenosových front klastru” na stránce 28
Zvolte mezi třemi režimy kontroly, když aplikace vkládá zprávy do vzdálených front klastru. Režimy vzdáleně kontrolují frontu klastru, lokálně kontrolují produkt `SYSTEM.CLUSTER.TRANSMIT.QUEUE`nebo lokální profily pro frontu klastru nebo správce front klastru.

Práce s přenosovými frontami klastru a odesílacími kanály klastru

“Překrývající se klastry” na stránce 34
Překrývající se klastry poskytují další administrativní schopnosti. Pomocí seznamů názvů snižte počet příkazů potřebných pro správu překrývajících se klastrů.

Související úlohy

Autorizace vkládání zpráv do front vzdáleného klastru

Přidání definice vzdálené fronty pro izolování zpráv odeslaných ze správce front brány

Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány

Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaných ze správce front brány

Změna výchozího nastavení na oddělení přenosových front klastru pro izolaci přenosu zpráv

Vytvoření dvou překrývajících se klastrů se správcem front brány

Konfigurace cest zpráv mezi klastry

Zabezpečení

Související odkazy

setmqaut

Klastrování: Plánování konfigurace přenosových front klastru
Budete provedeni pomocí voleb přenosových front klastru. Můžete konfigurovat jednu společnou výchozí frontu, samostatné výchozí fronty nebo ručně definované fronty.

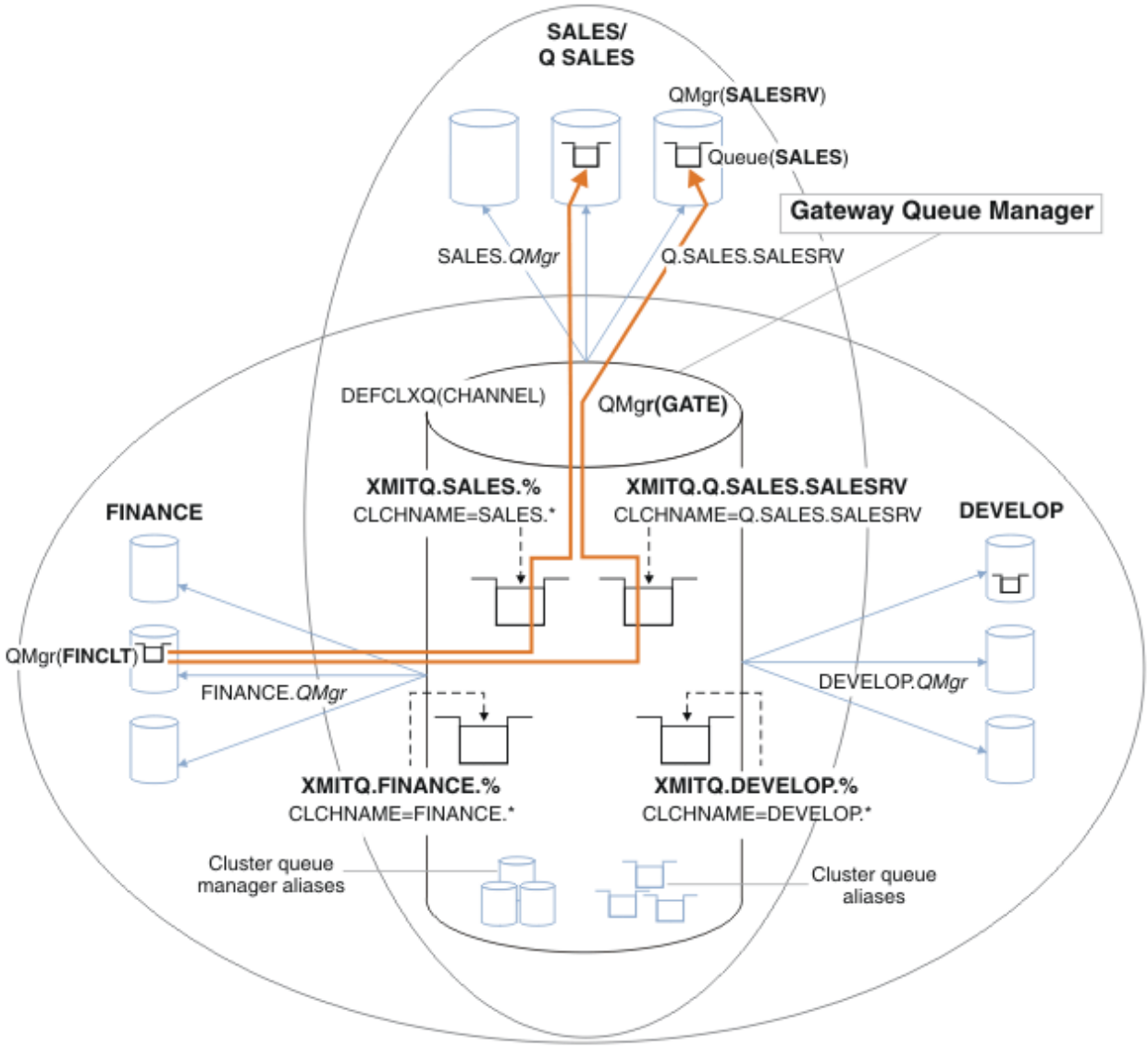
Než začnete

Přezkoumejte “Jak vybrat typ přenosové fronty klastru, který se má použít” na stránce 51.

Informace o této úloze

Při plánování konfigurace správce front pro výběr přenosové fronty klastru je třeba provést určité volby.

1. Jaká je výchozí přenosová fronta klastru pro přenosy zpráv klastru?
   a. Společná přenosová fronta klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.
   b. Oddělte přenosové fronty klastru. Správce front spravuje samostatné přenosové fronty klastru. Vytváří je jako trvalé dynamické fronty z modelové fronty `SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE`. Vytvoří jednu přenosovou frontu klastru pro každý odesílací kanál klastru, který používá.
2. Pro přenosové fronty klastru, které se rozhodnete vytvořit ručně, máte další dvě možnosti:
   a. Definujte samostatnou přenosovou frontu pro každý odesílací kanál klastru, který se rozhodnete konfigurovat ručně. V tomto případě nastavte atribut fronty **CLCHNAME** přenosové fronty na název odesílacího kanálu klastru. Vyberte odesílací kanál klastru, který má přenášet zprávy z této přenosové fronty.
   b. Kombinujte přenos zpráv pro skupinu odesílacích kanálů klastru do stejné přenosové fronty klastru; viz Obrázek 13 na stránce 50. V tomto případě nastavte atribut fronty **CLCHNAME** pro každou společnou přenosovou frontu na název kanálu odesilatele generického klastru. Generický název odesílacího kanálu klastru je filtr pro seskupení názvů odesílacích kanálů klastru. Například `SALES.*` seskupí všechny odesílací kanály klastru, které mají názvy začínající na `SALES.`. Kdekoli v řetězci filtru můžete umístit více zástupných znaků. Zástupným znakem je hvězdička "`*`". Představuje od nuly do libovolného počtu znaků.



Obrázek 13. Příklad specifických přenosových front pro různé klastry IBM MQ oddělení

Postup

1. Vyberte typ výchozí přenosové fronty klastru, která se má použít.
   - Zvolte jednu přenosovou frontu klastru nebo samostatné fronty pro každé připojení klastru.

   Ponechte výchozí nastavení nebo spusťte příkaz **MQSC** :

   ```
   ALTER QMGR DEFCLXQ(CHANNEL)
   ```

2. Izolujte všechny toky zpráv, které nesmí sdílet přenosovou frontu klastru s jinými toky.
   - Viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 53. V příkladu je fronta SALES , která musí být izolována, členem klastru SALES v systému SALESRV. Chcete-li izolovat frontu SALES , vytvořte nový klastr `Q.SALES`, učiňte správce front SALESRV členem a upravte frontu SALES tak, aby patřila do fronty `Q.SALES`.
   - Správci front, kteří odesílají zprávy do produktu SALES , musí být také členy nového klastru. Pokud použijete alias klastrované fronty a správce front brány, jako v tomto příkladu, můžete v mnoha případech omezit změny na to, aby se správce front brány stal členem nového klastru.

- Oddělení toků od brány k cíli však neodděluje toky k bráně od zdrojového správce front. Ale někdy se ukáže, že je dostatečné oddělit toky od brány a ne toky k bráně. Pokud to nestačí, přidejte zdrojového správce front do nového klastru. Chcete-li zprávy procházet bránou, přesuňte alias klastru do nového klastru a pokračujte v odesílání zpráv do aliasu klastru na bráně, nikoli přímo do cílového správce front.

Chcete-li izolovat toky zpráv, postupujte takto:

a) Nakonfigurujte cíle toků tak, aby každá cílová fronta byla jedinou frontou ve specifickém klastru v daném správci front.

b) Vytvořte kanály odesilatele a příjemce klastru pro všechny nové klastry, které jste vytvořili podle systematické konvence pojmenování.

- Viz “Klastrování: Zvláštní aspekty pro překrývající se klastry” na stránce 41.

c) Definujte přenosovou frontu klastru pro každé izolované místo určení v každém správci front, který odesílá zprávy do cílové fronty.

- Konvencí pojmenování pro přenosové fronty klastru je použití hodnoty atributu názvu kanálu klastru `CLCHNAME`s předponou `XMITQ.` .

3. Vytvořte přenosové fronty klastru tak, aby splňovaly požadavky na řízení nebo monitorování.

- Typické požadavky na řízení a monitorování vedou k přenosové frontě na klastr nebo přenosové frontě na správce front. Pokud dodržujete konvenci pojmenování pro kanály klastru *`ClusterName`*`.`*`QueueManagerName`*, je snadné vytvořit generické názvy kanálů, které vybírají klastr správců front, nebo všechny klastry, jejichž je správce front členem; viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 53.
- Rozšiřte konvence pojmenování pro přenosové fronty klastru tak, aby vyhovovaly generickým názvům kanálů, nahrazením symbolu hvězdičky znakem procenta. Například:

```
DEFINE QLOCAL(XMITQ.SALES.%) USAGE(XMITQ) CLCHNAME(SALES.*)
```

Související pojmy

Práce s přenosovými frontami klastru a odesílacími kanály klastru

“Řízení přístupu a více přenosových front klastru” na stránce 28

Zvolte mezi třemi režimy kontroly, když aplikace vkládá zprávy do vzdálených front klastru. Režimy vzdáleně kontrolují frontu klastru, lokálně kontrolují produkt `SYSTEM.CLUSTER.TRANSMIT.QUEUE`nebo lokální profily pro frontu klastru nebo správce front klastru.

“Překrývající se klastry” na stránce 34

Překrývající se klastry poskytují další administrativní schopnosti. Pomocí seznamů názvů snižte počet příkazů potřebných pro správu překrývajících se klastrů.

Související úlohy

Přidání definice vzdálené fronty pro izolování zpráv odeslaných ze správce front brány

Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány

Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaných ze správce front brány

Změna výchozího nastavení na oddělení přenosových front klastru pro izolaci přenosu zpráv

Vytvoření dvou překrývajících se klastrů se správcem front brány

Konfigurace cest zpráv mezi klastry

Jak vybrat typ přenosové fronty klastru, který se má použít

Jak vybrat mezi různými volbami konfigurace přenosové fronty klastru.

Můžete zvolit, která přenosová fronta klastru je přidružena k odesílacímu kanálu klastru.

1. Všechny odesílací kanály klastru mohou být přidruženy k jedné výchozí přenosové frontě klastru `SYSTEM.CLUSTER.TRANSMIT.QUEUE`; tato volba je výchozí.

2. Můžete nastavit, aby všechny odesílací kanály klastru byly automaticky přidruženy k oddělené přenosové frontě klastru. Fronty jsou vytvořeny správcem front z modelové fronty SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE s názvem SYSTEM.CLUSTER.TRANSMIT.*ChannelName*. Kanály budou používat svou přenosovou frontu klastru s jedinečným názvem, pokud je atribut správce front **DEFCLXQ** nastaven na hodnotu CHANNEL.
3. Můžete nastavit specifické odesílací kanály klastru tak, aby byly obsluhovány jednou přenosovou frontou klastru. Tuto volbu vyberte vytvořením přenosové fronty a nastavením jejího atributu **CLCHNAME** na název odesílacího kanálu klastru.
4. Můžete vybrat skupiny odesílacích kanálů klastru, které mají být obsluhovány jednou přenosovou frontou klastru. Tuto volbu vyberte vytvořením přenosové fronty a nastavením jejího atributu **CLCHNAME** na generický název kanálu, například *ClusterName*.*. Pokud pojmenujete kanály klastru podle konvencí pojmenování uvedených v části "Klastrování: Zvláštní aspekty pro překrývající se klastry" na stránce 41, tento název vybere všechny kanály klastru připojené ke správcům front v klastru *ClusterName*.

Můžete kombinovat jednu z výchozích voleb přenosové fronty klastru pro některé odesílací kanály klastru s libovolným počtem specifických a generických konfigurací přenosové fronty klastru.

Doporučené postupy

Ve většině případů je pro existující instalace produktu IBM MQ nejlepší volbou výchozí konfigurace. Správce front klastru ukládá zprávy klastru do jedné přenosové fronty klastru, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Máte možnost změnit výchozí nastavení ukládání zpráv pro různé správce front a různé klastry v samostatných přenosových frontách nebo definovat vlastní přenosové fronty.

Ve většině případů je pro nové instalace produktu IBM MQ nejlepší volbou také výchozí konfigurace. Proces přepnutí z výchozí konfigurace na alternativní výchozí nastavení s jednou přenosovou frontou pro každý odesílací kanál klastru je automatický. Přepínání zpět je také automatické. Volba jednoho nebo druhého není kritická, můžete ji zvrátit.

Důvodem pro výběr jiné konfigurace je spíše řízení a správa než funkčnost nebo výkon. S několika výjimkami konfigurace více přenosových front klastru neprospívá chování správce front. Výsledkem je více front a vyžaduje, abyste upravili procedury monitorování a správy, které jste již nastavili a které odkazují na jedinou přenosovou frontu. To je důvod, proč, v rovnováze, zůstat s výchozí konfigurací je nejlepší volbou, pokud nemáte silné řízení nebo řízení důvody pro jinou volbu.

Obě výjimky se týkají toho, co se stane, když se zvýší počet zpráv uložených v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE . Pokud podniknete každý krok k oddělení zpráv pro jeden cíl od zpráv pro jiný cíl, pak kanál a problémy s doručením s jedním cílem by neměly mít vliv na doručení do jiného místa určení. Počet zpráv uložených v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE se však může zvýšit kvůli tomu, že se zprávy nedoručují dostatečně rychle do jednoho místa určení. Počet zpráv v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE pro jedno místo určení může ovlivnit doručení zpráv do jiných míst určení.

Chcete-li se vyhnout problémům, které jsou důsledkem zaplnění jedné přenosové fronty, zaměřte se na vytvoření dostatečné kapacity do vaší konfigurace. Pokud dojde k selhání místa určení a začne se sestavovat seznam nevyřízených zpráv, máte čas na opravu problému.

Jsou-li zprávy směrovány prostřednictvím správce front rozbočovače, například prostřednictvím brány klastru, sdílejí společnou přenosovou frontu SYSTEM.CLUSTER.TRANSMIT.QUEUE. Pokud počet zpráv uložených v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE ve správci front brány dosáhne maximální hloubky, začne správce front odmítat nové zprávy pro přenosovou frontu, dokud se jejich hloubka nezmenší. Zahlcení ovlivňuje zprávy pro všechna místa určení, která jsou směrována přes bránu. Zprávy zálohujte přenosové fronty jiných správců front, kteří odesílají zprávy bráně. Problém se projevuje ve zprávách zapisovaných do protokolů chyb správce front, s klesající propustností zpráv a s delšími uplynulými dobami mezi odesláním zprávy a časem, kdy zpráva dorazila do místa určení.

Vliv zahlcení na jednu přenosovou frontu se může projevit i před jejím zaplněním. Máte-li smíšený přenos zpráv, s některými velkými dočasnými zprávami a některými malými zprávami, čas na doručení malých

zpráv se zvyšuje s tím, jak se plní přenosová fronta. Prodleva je způsobena zápisem velkých přechodných zpráv na disk, které by normálně nebyly zapsány na disk. Máte-li časové kritické toky zpráv a sdílíte-li přenosovou frontu klastru s jinými smíšenými toky zpráv, může být vhodné konfigurovat speciální cestu ke zprávám, abyste ji izolovali od ostatních toků zpráv. Viz Přidání klastru a přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány.

Další důvody pro konfiguraci samostatných přenosových front klastru jsou splnění požadavků na řízení nebo zjednodušení monitorování zpráv odesílaných do různých cílů klastru. Můžete například prokázat, že zprávy pro jedno místo určení nikdy nesdílely přenosovou frontu se zprávami pro jiné místo určení.

Chcete-li vytvořit různé přenosové fronty klastru pro každý odesílací kanál klastru, změňte atribut správce front **DEFCLXQ** , který řídí výchozí přenosovou frontu klastru. Odesílací kanál klastru může sdílet více míst určení, takže musíte klastry naplánovat tak, aby tento cíl plně splňovaly. Metodu Přidání klastru a přenosové fronty klastru pro systematickou izolaci provozu zpráv klastru odeslaných ze správce front brány použijte pro všechny fronty klastru. Výsledkem, o který se snažíte, je, aby žádný cíl klastru nesdílel odesílací kanál klastru s jiným cílem klastru. V důsledku toho žádná zpráva pro místo určení klastru nesdílí svou přenosovou frontu klastru se zprávou pro jiné místo určení.

Vytvoření samostatné přenosové fronty klastru pro určitý tok zpráv usnadňuje monitorování toku zpráv do tohoto místa určení. Chcete-li použít novou přenosovou frontu klastru, definujte ji, přidružte ji k odesílacímu kanálu klastru a zastavte a spusťte kanál. Změna nemusí být trvalá. Můžete izolovat tok zpráv na chvíli, monitorovat přenosovou frontu a pak se znovu vrátit k použití výchozí přenosové fronty.

Související úlohy

Klastrování: Příklad konfigurace více přenosových front klastru
V této úloze použijete kroky k plánování více přenosových front klastru na tři překrývající se klastry. Požadavky jsou na oddělení toků zpráv do jedné fronty klastru, od všech ostatních toků zpráv a na uložení zpráv pro různé klastry v různých přenosových frontách klastru.

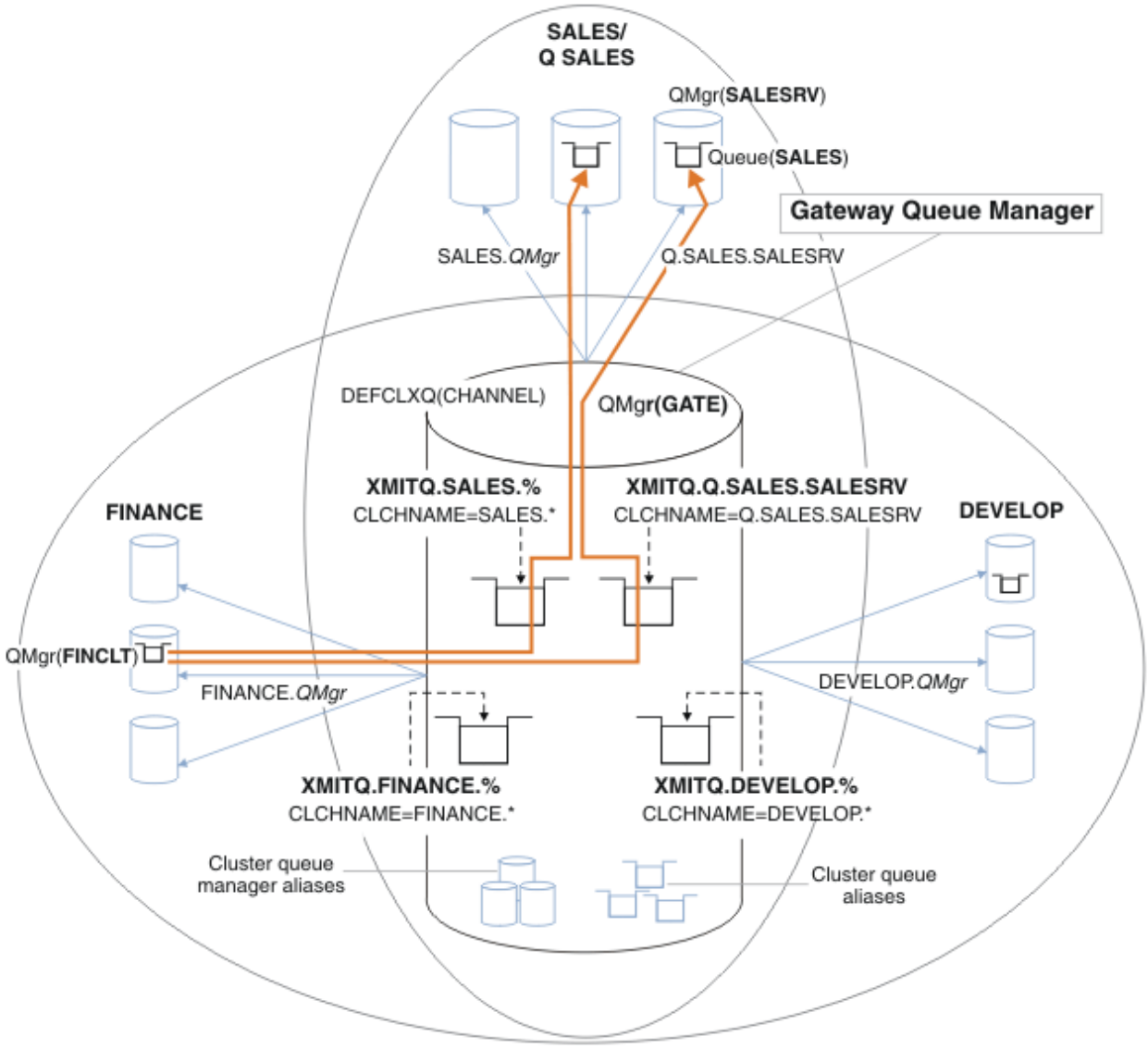
Klastrování: Přepínání přenosových front klastru
Naplánujte, jak se projeví změny v přenosových frontách klastru existujícího produkčního správce front.

Klastrování: Příklad konfigurace více přenosových front klastru
V této úloze použijete kroky k plánování více přenosových front klastru na tři překrývající se klastry. Požadavky jsou na oddělení toků zpráv do jedné fronty klastru, od všech ostatních toků zpráv a na uložení zpráv pro různé klastry v různých přenosových frontách klastru.

Informace o této úloze

Kroky v této úloze ukazují, jak použít proceduru v produktu “Klastrování: Plánování konfigurace přenosových front klastru” na stránce 48 a jak dorazit do konfigurace zobrazené v souboru Obrázek 14 na stránce 54. Jedná se o příklad tří překrývajících se klastrů se správcem front brány, který je konfigurován se samostatnými přenosovými frontami klastru. Příkazy MQSC pro definování klastrů jsou popsány v tématu “Vytvoření ukázkového klastru” na stránce 56.

V tomto příkladu existují dva požadavky. Jedním z nich je oddělit tok zpráv od správce front brány do prodejní aplikace, která protokoluje prodej. Druhým je dotazovat se, kolik zpráv čeká na odeslání do různých oblastí oddělení v libovolném časovém okamžiku. Klastry `SALES`, `FINANCE`a `DEVELOP` jsou již definovány. Zprávy klastru jsou momentálně postoupeny z `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.



Obrázek 14. Příklad specifických přenosových front pro různé klastry IBM MQ oddělení

Postup úpravy klastrů je následující. Definice viz Změny pro izolaci prodejní fronty v novém klastru a oddělení přenosových front klastru brány.

Postup

1. Prvním krokem konfigurace je " Vyberte typ výchozí přenosové fronty klastru, která se má použít ".

   Rozhodnutí je vytvořit oddělené výchozí přenosové fronty klastru spuštěním následujícího příkazu **MQSC** ve správci front GATE .

   ```
   ALTER QMGR DEFCLXQ(CHANNEL)
   ```

   Neexistuje žádný silný důvod pro výběr tohoto výchozího nastavení, protože záměrem je ručně definovat přenosové fronty klastru. Volba má slabou diagnostickou hodnotu. Pokud je ruční definice provedena nesprávně a zpráva prochází výchozí přenosovou frontou klastru, zobrazí se při vytváření přenosové fronty trvalého dynamického klastru.
2. Druhým krokem konfigurace je " Izolujte všechny toky zpráv, které nesmí sdílet přenosovou frontu klastru s jinými toky ".

V tomto případě prodejní aplikace, která přijímá zprávy z fronty SALES v systému SALESRV , vyžaduje izolaci. Je vyžadována pouze izolace zpráv od správce front brány. Tyto tři dílčí kroky jsou:

a) " Nakonfigurujte cíle toků tak, aby každá cílová fronta byla jedinou frontou ve specifickém klastru v daném správci front ".

Příklad vyžaduje přidání správce front SALESRV do nového klastru v rámci obchodního oddělení. Máte-li několik front, které vyžadují izolaci, můžete rozhodnout o vytvoření specifického klastru pro frontu SALES . Možná konvence pojmenování pro název klastru je pojmenovat takové klastry, `Q.`*`QueueName`*, například `Q.SALES`. Alternativním přístupem, který může být praktičtější, pokud máte velký počet front, které mají být izolovány, je vytvořit klastry izolovaných front, kde a v případě potřeby. Názvy klastrů mohou být `QUEUES.` *n*.

V tomto příkladu se nový klastr nazývá `Q.SALES`. Chcete-li přidat nový klastr, prohlédněte si definice v části Změny pro izolování prodejní fronty v novém klastru a oddělení přenosových front klastru brány. Souhrn změn definice je následující:

i) Přidejte `Q.SALES` do seznamu názvů klastrů ve správcích front úložiště. Na seznam názvů se odkazuje v parametru **REPOSNL** správce front.

ii) Přidejte `Q.SALES` do seznamu názvů klastrů ve správci front brány. Seznam názvů je odkazován ve všech definicích aliasu fronty klastru a aliasu správce front klastru ve správci front brány.

iii) Vytvořte seznam názvů ve správci front SALESRVpro klastry, jejichž je členem, a změňte členství v klastru fronty SALES :

```
DEFINE NAMELIST(CLUSTERS) NAMES(SALES, Q.SALES) REPLACE
ALTER QLOCAL(SALES) CLUSTER(' ') CLUSNL(SALESRV.CLUSTERS)
```

Fronta SALES je členem obou klastrů, pouze pro přechod. Po spuštění nové konfigurace odeberte frontu SALES z klastru SALES ; viz Obrázek 15 na stránce 59.

b) " Vytvořte kanály odesilatele a příjemce klastru pro všechny nové klastry, které jste vytvořili podle systematické konvence pojmenování ".

i) Přidejte kanál příjemce klastru `Q.SALES.` *`RepositoryQMgr`* do všech správců front úložiště.

ii) Přidejte kanál odesilatele klastru `Q.SALES.` *`OtherRepositoryQMgr`* do všech správců front úložiště, abyste se připojili k druhému správci úložiště. Spusťte tyto kanály.

iii) Přidejte přijímací kanály klastru `Q.SALES.SALESRV`a `Q.SALES.GATE` do jednoho ze spuštěných správců front úložiště.

iv) Přidejte odesílací kanály klastru `Q.SALES.SALESRV`a `Q.SALES.GATE` do správců front SALESRV a GATE . Připojte odesílací kanál klastru ke správci front úložiště, na kterém jste vytvořili přijímací kanály klastru.

c) " Definujte přenosovou frontu klastru pro každé izolované místo určení v každém správci front, který odesílá zprávy do cílové fronty ".

Ve správci front brány definujte přenosovou frontu klastru `XMITQ.Q.SALES.SALESRV` pro odesílací kanál klastru `Q.SALES.SALESRV` :

```
DEFINE QLOCAL(XMITQ.Q.SALES.SALESRV) USAGE(XMITQ) CLCHNAME(Q.SALES.SALESRV) REPLACE
```

3. Třetím krokem konfigurace je " Vytvořte přenosové fronty klastru tak, aby splňovaly požadavky na řízení nebo monitorování ".

Ve správci front brány definujte přenosové fronty klastru:

```
DEFINE QLOCAL(XMITQ.SALES)  USAGE(XMITQ) CLCHNAME(SALES.*)  REPLACE
DEFINE QLOCAL(XMITQ.DEVELOP) USAGE(XMITQ) CLCHNAME(DEVELOP.*) REPLACE
DEFINE QLOCAL(XMITQ.FINANCE) USAGE(XMITQ) CLCHNAME(SALES.*)  REPLACE
```

Jak pokračovat dále

Přepněte na novou konfiguraci ve správci front brány.

Přepínač se spustí spuštěním nových kanálů a restartováním kanálů, které jsou nyní přidruženy k různým přenosovým frontám. Případně můžete zastavit a spustit správce front brány.

1. Zastavte následující kanály ve správci front brány:

```
SALES. Qmgr
DEVELOP. Qmgr
FINANCE. Qmgr
```

2. Spusťte následující kanály ve správci front brány:

```
SALES. Qmgr
DEVELOP. Qmgr
FINANCE. Qmgr
Q.SALES.SAVESRV
```

Po dokončení přepínače odeberte frontu SALES z klastru SALES ; viz Obrázek 15 na stránce 59.

Související pojmy

Jak vybrat typ přenosové fronty klastru, který se má použít
Jak vybrat mezi různými volbami konfigurace přenosové fronty klastru.

Související úlohy

Klastrování: Přepínání přenosových front klastru
Naplánujte, jak se projeví změny v přenosových frontách klastru existujícího produkčního správce front.

Vytvoření ukázkového klastru
Definice a pokyny pro vytvoření vzorového klastru a jeho úpravu za účelem izolování fronty SALES a samostatných zpráv ve správci front brány.

Informace o této úloze

Úplné příkazy **MQSC** pro vytvoření klastrů FINANCE, SALESa Q.SALES jsou uvedeny v části Definice pro základní klastry, Změny pro izolování prodejní fronty v novém klastru a oddělení přenosových front klastru bránya Odebrání prodejní fronty ve správci front SALESRV z prodejního klastru. Klastr DEVELOP je vynechán z definic, aby byly definice kratší.

Postup

1. Vytvořte klastry SALES a FINANCE a správce front brány.
   a) Vytvořte správce front.

      Spusťte příkaz: `crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE` *QmgrName* pro každý název správce front v adresáři Tabulka 4 na stránce 56.

Tabulka 4. Názvy správců front a čísla portů		
Popis	**Název správce front**	**Číslo portu**
Finanční úložiště	FINR1	1414
Finanční úložiště	FINR2	1415
Finanční klient	FINCLT	1418
Prodejní úložiště	SALER1	1416
Prodejní úložiště	SALER2	1417
Prodejní server	SALESRV	1419

Tabulka 4. Názvy správců front a čísla portů (pokračování)		
Popis	**Název správce front**	**Číslo portu**
Komunikační brána	GATE	1420

b) Spustit všechny správce front

Spusťte příkaz: `strmqm` *QmgrName* pro každý název správce front v adresáři Tabulka 4 na stránce 56.

c) Vytvořit definice pro každého ze správců front

Spusťte příkaz: `runmqsc` *QmgrName* < *filename* , kde jsou soubory uvedeny v části Definice pro základní klastrya název souboru odpovídá názvu správce front.

Definice pro základní klastry
finr1.txt

```
DEFINE LISTENER(1414) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1414) REPLACE
START LISTENER(1414)
ALTER QMGR REPOS(FINANCE)
DEFINE CHANNEL(FINANCE.FINR2) CHLTYPE(CLUSSDR) CONNAME('localhost(1415)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1414)')
CLUSTER(FINANCE) REPLACE
```

finr2.txt

```
DEFINE LISTENER(1415) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1415) REPLACE
START LISTENER(1415)
ALTER QMGR REPOS(FINANCE)
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSSDR) CONNAME('localhost(1414)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.FINR2) CHLTYPE(CLUSRCVR) CONNAME('localhost(1415)')
CLUSTER(FINANCE) REPLACE
```

finclt.txt

```
DEFINE LISTENER(1418) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1418) REPLACE
START LISTENER(1418)
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSSDR)  CONNAME('localhost(1414)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.FINCLT) CHLTYPE(CLUSRCVR) CONNAME('localhost(1418)')
CLUSTER(FINANCE) REPLACE
DEFINE QMODEL(SYSTEM.SAMPLE.REPLY) REPLACE
```

saler1.txt

```
DEFINE LISTENER(1416) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1416) REPLACE
START LISTENER(1416)
ALTER QMGR REPOS(SALES)
DEFINE CHANNEL(SALES.SALER2) CHLTYPE(CLUSSDR) CONNAME('localhost(1417)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1416)')
CLUSTER(SALES) REPLACE
```

saler2.txt

```
DEFINE LISTENER(1417) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1417) REPLACE
START LISTENER(1417)
ALTER QMGR REPOS(SALES)
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.SALER2) CHLTYPE(CLUSRCVR) CONNAME('localhost(1417)')
CLUSTER(SALES) REPLACE
```

salesrv.txt

```
DEFINE LISTENER(1419) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1419) REPLACE
START LISTENER(1419)
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.SALESRV) CHLTYPE(CLUSRCVR) CONNAME('localhost(1419)')
CLUSTER(SALES) REPLACE
DEFINE QLOCAL(SALES) CLUSTER(SALES) TRIGGER INITQ(SYSTEM.DEFAULT.INITIATION.QUEUE)
PROCESS(ECHO) REPLACE
DEFINE PROCESS(ECHO) APPLICID(AMQSECH) REPLACE
```

gate.txt

```
DEFINE LISTENER(1420) TRPTYPE(TCP) IPADDR(LOCALHOST) CONTROL(QMGR) PORT(1420) REPLACE
START LISTENER(1420)
DEFINE NAMELIST(ALL) NAMES(SALES, FINANCE)
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSSDR) CONNAME('LOCALHOST(1414)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.GATE) CHLTYPE(CLUSRCVR) CONNAME('LOCALHOST(1420)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('LOCALHOST(1416)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.GATE)  CHLTYPE(CLUSRCVR) CONNAME('LOCALHOST(1420)')
CLUSTER(SALES) REPLACE
DEFINE QALIAS(A.SALES) CLUSNL(ALL) TARGET(SALES) TARGTYPE(QUEUE) DEFBIND(NOTFIXED)
REPLACE
DEFINE QREMOTE(FINCLT) RNAME(' ') RQMNAME(FINCLT) CLUSNL(ALL) REPLACE
DEFINE QREMOTE(SALESRV) RNAME(' ') RQMNAME(SALESRV) CLUSNL(ALL) REPLACE
```

2. Otestujte konfiguraci spuštěním ukázkového programu požadavků.
   a) Spuštění programu monitoru spouštěčů ve správci front SALESRV

      V systému Windowsotevřete příkazové okno a spusťte příkaz `runmqtrm -m SALESRV`

   b) Spusťte ukázkový program požadavků a odešlete požadavek.

      V systému Windowsotevřete příkazové okno a spusťte příkaz `amqsreq A.SALES FINCLT`

      Zpráva požadavku se vrátí zpět a po 15 sekundách se ukázkový program dokončí.
3. Vytvořte definice pro izolaci fronty SALES v klastru `Q.SALES` a samostatné zprávy klastru pro klastr SALES a FINANCE ve správci front brány.

   Spusťte příkaz: `runmqsc` *QmgrName* < *filename* , kde jsou soubory uvedeny v následujícím seznamu, a název souboru se téměř shoduje s názvem správce front.

   Změny pro izolaci prodejní fronty v novém klastru a oddělení přenosových front klastru brány
   chgsaler1.txt

```
DEFINE NAMELIST(CLUSTERS) NAMES(SALES, Q.SALES)
ALTER QMGR REPOS(' ') REPOSNL(CLUSTERS)
DEFINE CHANNEL(Q.SALES.SALER2) CHLTYPE(CLUSSDR) CONNAME('localhost(1417)')
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
```

   chgsaler2.txt

```
DEFINE NAMELIST(CLUSTERS) NAMES(SALES, Q.SALES)
ALTER QMGR REPOS(' ') REPOSNL(CLUSTERS)
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.SALER2) CHLTYPE(CLUSRCVR) CONNAME('localhost(1417)')
CLUSTER(Q.SALES) REPLACE
```

   chgsalesrv.txt

```
DEFINE NAMELIST (CLUSTERS) NAMES(SALES, Q.SALES)
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
```

```
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.SAVESRV) CHLTYPE(CLUSRCVR) CONNAME('localhost(1419)')
CLUSTER(Q.SALES) REPLACE
ALTER QLOCAL (SALES) CLUSTER(' ') CLUSNL(CLUSTERS)
```

chggate.txt

```
ALTER NAMELIST(ALL) NAMES(SALES, FINANCE, Q.SALES)
ALTER QMGR DEFCLXQ(CHANNEL)
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSSDR)  CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.GATE)  CHLTYPE(CLUSRCVR) CONNAME('localhost(1420)')
CLUSTER(Q.SALES) REPLACE
DEFINE QLOCAL (XMITQ.Q.SALES.SALESRV) USAGE(XMITQ) CLCHNAME(Q.SALES.SALESRV) REPLACE
DEFINE QLOCAL (XMITQ.SALES)     USAGE(XMITQ) CLCHNAME(SALES.*)  REPLACE
DEFINE QLOCAL (XMITQ.FINANCE)    USAGE(XMITQ) CLCHNAME(FINANCE.*) REPLACE
```

4. Odeberte frontu SALES z klastru SALES .

   Spusťte příkaz **MQSC** v adresáři Obrázek 15 na stránce 59:

   ```
   ALTER QLOCAL(SALES) CLUSTER('Q.SALES') CLUSNL(' ')
   ```

   Obrázek 15. Odebrat prodejní frontu ve správci front SALESRV z prodejního klastru

5. Přepněte kanály do nových přenosových front.

   Požadavkem je zastavit a spustit všechny kanály, které používá správce front GATE . Chcete-li to provést s nejmenším počtem příkazů, zastavte a spusťte správce front.

   ```
   endmqm -i GATE
   strmqm GATE
   ```

Jak pokračovat dále

1. Znovu spusťte ukázkový program požadavků, abyste ověřili, že nová konfigurace funguje; viz krok “2” na stránce 58
2. Monitorujte zprávy procházející všemi přenosovými frontami klastru ve správci front GATE :
   a. Změňte definici každé z přenosových front klastru tak, aby bylo zapnuté monitorování front.

      ```
      ALTER QLOCAL(SYSTEM.CLUSTER.TRANSMIT.
      name) STATQ(ON)
      ```

   b. Zkontrolujte, zda je monitorování statistiky správce front OFF, abyste minimalizovali výstup, a nastavte interval monitorování na nižší hodnotu, abyste mohli pohodlně provádět více testů.

      ```
      ALTER QMGR STATINT(60) STATCHL(OFF) STATQ(OFF) STATMQI(OFF) STATACLS(OFF)
      ```

   c. Restartujte správce front GATE .
   d. Několikrát spusťte ukázkový program požadavků, abyste ověřili, že přes SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV a SYSTEM.CLUSTER.TRANSMIT.QUEUEprotéká stejný počet zpráv. Požadavky procházejí produktem SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV a odpovědi procházejí produktem SYSTEM.CLUSTER.TRANSMIT.QUEUE.

      ```
      amqsmon -m GATE -t statistics
      ```

   e. Výsledky v několika intervalech jsou následující:

```
C:\Documents and Settings\Admin>amqsmon -m GATE -t statistics
MonitoringType: QueueStatistics
QueueManager: 'GATE'
IntervalStartDate: '2012-02-27'
IntervalStartTime: '14.59.20'
IntervalEndDate: '2012-02-27'
IntervalEndTime: '15.00.20'
CommandLevel: 700
ObjectCount: 2
QueueStatistics: 0
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.QUEUE'
CreateDate: '2012-02-24'
CreateTime: '15.58.15'
...
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [435, 0]
GetCount: [1, 0]
GetBytes: [435, 0]
...
QueueStatistics: 1
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV'
CreateDate: '2012-02-24'
CreateTime: '16.37.43'
...
PutCount: [1, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [435, 0]
GetCount: [1, 0]
GetBytes: [435, 0]
...
MonitoringType: QueueStatistics
QueueManager: 'GATE'
IntervalStartDate: '2012-02-27'
IntervalStartTime: '15.00.20'
IntervalEndDate: '2012-02-27'
IntervalEndTime: '15.01.20'
CommandLevel: 700
ObjectCount: 2
QueueStatistics: 0
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.QUEUE'
CreateDate: '2012-02-24'
CreateTime: '15.58.15'
...
PutCount: [2, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [863, 0]
GetCount: [2, 0]
GetBytes: [863, 0]
...
QueueStatistics: 1
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV'
CreateDate: '2012-02-24'
CreateTime: '16.37.43'
```

```
...
PutCount: [2, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [863, 0]
GetCount: [2, 0]
GetBytes: [863, 0]
...
2 Records Processed.
```

Jedna zpráva požadavku a odpovědi byla odeslána v prvním intervalu a dvě ve druhém. Můžete odvodit, že zprávy požadavků byly umístěny v systému SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV, a zprávy odpovědí v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Klastrování: Přepínání přenosových front klastru
Naplánujte, jak se projeví změny v přenosových frontách klastru existujícího produkčního správce front.

Než začnete

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přepínání se dokončí rychleji. Přečtěte si téma Jak proces přepnutí odesílacího kanálu klastru na jinou přenosovou frontu funguje , abyste se před dalším pokračováním pokusili přenosovou frontu vyprázdnit.

Informace o této úloze

Máte na výběr ze dvou způsobů, jak se projeví změny v přenosových frontách klastru.

1. Nechte správce front provést změny automaticky. Toto nastavení je výchozí. Správce front přepne odesílací kanály klastru s nevyřízenými změnami přenosové fronty při příštím spuštění odesílacího kanálu klastru.
2. Proveďte změny ručně. Při zastavení kanálu odesilatele klastru můžete provést změny. Před spuštěním odesílacího kanálu klastru jej můžete přepnout z jedné přenosové fronty klastru na jinou.

Jaké faktory zohledňujete při rozhodování o tom, kterou ze dvou možností zvolit, a jak spravujete přepínač?

Procedura

- Volba 1: Nechte správce front provést změny automaticky; viz “Přepnutí aktivních odesílacích kanálů klastru na jinou sadu přenosových front klastru” na stránce 62.

  Tuto volbu vyberte, chcete-li, aby správce front provedl přepnutí za vás.

  Alternativním způsobem, jak popsat tuto volbu, je říci, že správce front přepne odesílací kanál klastru, aniž byste museli vynutit zastavení kanálu. Máte možnost vynutit zastavení kanálu a následné spuštění kanálu, aby se přepnutí stalo dříve. Přepínač se spustí při spuštění kanálu a spustí se, když je kanál spuštěn, což se liší od volby 2. Ve volbě 2 se přepínač provede při zastavení kanálu.

  Vyberete-li tuto volbu tak, že umožníte automatické spuštění přepínače, spustí se proces přepínání při spuštění odesílacího kanálu klastru. Není-li kanál zastaven, spustí se po jeho deaktivaci, dojde-li ke zpracování zprávy. Je-li kanál zastaven, spusťte jej pomocí příkazu START CHANNEL .
  Proces přepnutí se dokončí, jakmile pro kanál odesilatele klastru v přenosové frontě, kterou kanál obsluhoval, nezbývají žádné zprávy. Jakmile k tomu dojde, jsou nově příchozí zprávy pro odesílací kanál klastru uloženy přímo do nové přenosové fronty. Do té doby jsou zprávy uloženy ve staré přenosové frontě a přepínací proces přenáší zprávy ze staré přenosové fronty do nové přenosové fronty. Odesílací kanál klastru předává zprávy z nové přenosové fronty klastru během celého procesu přepínání.

Po dokončení procesu přepnutí závisí na stavu systému. Pokud provedete změny v okně údržby, předem zhodnoťte, zda bude proces přepínání dokončen včas. To, zda bude dokončeno v čase, závisí na tom, zda počet zpráv, které čekají na přenos ze staré přenosové fronty, dosáhne nuly.

Výhodou první metody je automatická. Nevýhodou je, že pokud je čas na provedení změn konfigurace omezen na okno údržby, musíte si být jisti, že můžete řídit systém, abyste dokončili proces přepnutí v okně údržby. Pokud si nemůžete být jisti, volba 2 může být lepší volbou.

- Volba 2: Proveďte změny ručně; viz "Přepnutí zastaveného odesílacího kanálu klastru na jinou přenosovou frontu klastru" na stránce 63.

  Tuto volbu vyberte, chcete-li řídit celý proces přepínání ručně nebo chcete-li přepnout zastavený nebo neaktivní kanál. Je to dobrá volba, pokud přepínáte několik odesílacích kanálů klastru a chcete provést přepnutí během okna údržby.

  Alternativním popisem této volby je, že přepínáte odesílací kanál klastru, zatímco je odesílací kanál klastru zastaven.

  Vyberete-li tuto volbu, budete mít úplnou kontrolu nad tím, kdy dojde k přepnutí.
  Můžete si být jisti dokončením procesu přepínání v pevném časovém úseku v rámci okna údržby. Doba, kterou přepínač zabere, závisí na tom, kolik zpráv má být přeneseno z jedné přenosové fronty do druhé. Pokud jsou zprávy stále doručovány, může procesu trvat určitou dobu, než přenese všechny zprávy.
  Máte možnost přepnout kanál bez přenosu zpráv ze staré přenosové fronty. Přepínač je "okamžitý".
  Když restartujete odesílací kanál klastru, začne zpracovávat zprávy v přenosové frontě, kterou jste k němu nově přiřadili.

  Výhodou druhé metody je, že máte kontrolu nad procesem přepínání. Nevýhodou je, že musíte identifikovat odesílací kanály klastru, které mají být přepnuty, spustit nezbytné příkazy a vyřešit všechny neověřené kanály, které by mohly bránit zastavení odesílacího kanálu klastru.

Související pojmy

Jak vybrat typ přenosové fronty klastru, který se má použít
Jak vybrat mezi různými volbami konfigurace přenosové fronty klastru.

Jak proces přepnutí odesílacího kanálu klastru na jinou přenosovou frontu pracuje

Související úlohy

Klastrování: Příklad konfigurace více přenosových front klastru
V této úloze použijete kroky k plánování více přenosových front klastru na tři překrývající se klastry. Požadavky jsou na oddělení toků zpráv do jedné fronty klastru, od všech ostatních toků zpráv a na uložení zpráv pro různé klastry v různých přenosových frontách klastru.

Přepnutí aktivních odesílacích kanálů klastru na jinou sadu přenosových front klastru
Tato úloha poskytuje tři možnosti přepínání aktivních odesílacích kanálů klastru. Jednou z možností je nechat správce front provést přepínač automaticky, což nemá vliv na spuštěné aplikace. Další volby jsou ruční zastavení a spuštění kanálů nebo restartování správce front.

Než začnete

Změňte konfiguraci přenosové fronty klastru. Můžete změnit atribut správce front **DEFCLXQ** nebo přidat či upravit atribut **CLCHNAME** přenosových front.

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přepínání se dokončí rychleji. Přečtěte si téma Jak proces přepnutí odesílacího kanálu klastru na jinou přenosovou frontu funguje , abyste se před dalším pokračováním pokusili přenosovou frontu vyprázdnit.

Informace o této úloze

Kroky v úloze použijte jako základ pro vypracování vlastního plánu pro provedení změn konfigurace přenosové fronty klastru.

Postup

1. Volitelné: Zaznamenat aktuální stav kanálu

   Vytvořte záznam stavu aktuálních a uložených kanálů, které obsluhují přenosové fronty klastru. Následující příkazy zobrazují stav přidružený k přenosovým frontám systémového klastru. Přidejte vlastní příkazy pro zobrazení stavu přidruženého k vámi definovaným přenosovým frontám klastru. Použijte konvenci, jako např. XMITQ. *ChannelName*, k pojmenování přenosových front klastru, které definujete, abyste usnadnili zobrazení stavu kanálu pro tyto přenosové fronty.

   ```
   DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
   DISPLAY CHSTATUS(*) SAVED WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
   ```

2. Přepnout přenosové fronty.

   - Nedělej nic. Správce front přepne odesílací kanály klastru při restartování po zastavení nebo deaktivaci.

     Tuto volbu vyberte, pokud nemáte žádná pravidla nebo obavy o změnu konfigurace správce front. Spuštěné aplikace nejsou změnami ovlivněny.
   - Restartujte správce front. Všechny odesílací kanály klastru jsou na vyžádání automaticky zastaveny a restartovány.

     Tuto volbu vyberte, chcete-li okamžitě zahájit všechny změny. Spuštěné aplikace jsou přerušeny správcem front při jeho ukončení a restartování.
   - Zastavte jednotlivé odesílací kanály klastru a restartujte je.

     Tuto volbu vyberte, chcete-li okamžitě změnit několik kanálů. U spuštěných aplikací dochází k krátké prodlevě v přenosu zpráv mezi zastavením a opětovným spuštěním kanálu zpráv. Odesílací kanál klastru zůstává spuštěn, s výjimkou doby, kdy jste jej zastavili. Během procesu přepínače jsou zprávy doručeny do staré přenosové fronty, přeneseny do nové přenosové fronty procesem přepínání a předány z nové přenosové fronty odesílacím kanálem klastru.

3. Volitelné: Monitorování kanálů při přepínání

   Zobrazit stav kanálu a hloubku přenosové fronty během přepínače. Následující příklad zobrazuje stav pro přenosové fronty systémového klastru.

   ```
   DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
   DISPLAY CHSTATUS(*) SAVED WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
   DISPLAY QUEUE('SYSTEM.CLUSTER.TRANSMIT.*') CURDEPTH
   ```

4. Volitelné: Monitorujte zprávy AMQ7341 Přenosové fronta pro kanál *ChannelName* přepínané z fronty *QueueName* na *QueueName* , které jsou zapsány do protokolu chyb správce front.

Přepnutí zastaveného odesílacího kanálu klastru na jinou přenosovou frontu klastru
Pokud se rozhodnete provést změny ručně, proveďte změny odesílacího kanálu klastru, když je zastaven, a přepněte jej z jedné přenosové fronty klastru do jiné před spuštěním odesílacího kanálu klastru.

Než začnete

Můžete provést některé změny konfigurace a nyní je chcete provést bez spuštění kanálů odesilatele klastru, které jsou ovlivněny. Případně můžete provést požadované změny konfigurace jako jeden z kroků v úloze.

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přepínání se dokončí rychleji. Přečtěte si téma Jak proces přepnutí odesílacího kanálu klastru na jinou přenosovou frontu funguje , abyste se před dalším pokračováním pokusili přenosovou frontu vyprázdnit.

Informace o této úloze

Tato úloha přepíná přenosové fronty obsluhované zastavenými nebo neaktivními odesílacími kanály klastru. Tuto úlohu můžete provést, protože je kanál odesilatele klastru zastaven a chcete okamžitě přepnout jeho přenosovou frontu. Například z nějakého důvodu se odesílací kanál klastru nespouští nebo má nějaký jiný problém s konfigurací. Chcete-li problém vyřešit, rozhodnete se vytvořit odesílací kanál klastru a přidružit přenosovou frontu pro starý odesílací kanál klastru k novému odesílacímu kanálu klastru, který jste definovali.

Pravděpodobnějším scénářem je, že chcete řídit, kdy se provádí opětovná konfigurace přenosových front klastru. Chcete-li plně řídit opětovnou konfiguraci, zastavte kanály, změňte konfiguraci a pak přepněte přenosové fronty.

Postup

1. Zastavte kanály, které chcete přepínat.
   a) Zastavte všechny spuštěné nebo neaktivní kanály, které chcete přepnout. Zastavení neaktivního odesílacího kanálu klastru zabrání jeho spuštění při provádění změn konfigurace.

   ```
   STOP CHANNEL(ChannelName) MODE(QUIESCSE) STATUS(STOPPED)
   ```

2. Volitelné: Proveďte změny konfigurace.

   Viz například “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 53.
3. Přepněte odesílací kanály klastru do nových přenosových front klastru.

   Multi V systému Multiplatformszadejte následující příkaz:

   ```
   runswchl -m QmgrName -c ChannelName
   ```

   z/OS V systému z/OSmůžete pomocí funkce SWITCH příkazu CSQUTIL přepínat zprávy nebo monitorovat, co se děje. Použijte následující příkaz.

   ```
   SWITCH CHANNEL(channel_name) MOVEMSGS(YES)
   ```

   Další informace viz Funkce SWITCH.

   Příkaz **runswchl**nebo CSQUTIL SWITCH přenese všechny zprávy ve staré přenosové frontě do nové přenosové fronty. Když počet zpráv ve staré přenosové frontě pro tento kanál dosáhne nuly, přepínač se dokončí. Příkaz je synchronní. Příkaz zapisuje zprávy o průběhu do okna během procesu přepínání.

   Během fáze přenosu jsou do nové přenosové fronty přeneseny existující a nové zprávy určené pro odesílací kanál klastru.

   Vzhledem k tomu, že je kanál odesilatele klastru zastaven, zprávy se sestavují v nové přenosové frontě. Chcete-li provést krok “2” na stránce 63 v souboru “Přepnutí aktivních odesílacích kanálů klastru na jinou sadu přenosových front klastru” na stránce 62, kontrastuje se zastavený kanál odesilatele klastru. V tomto kroku je kanál odesilatele klastru spuštěn, takže zprávy nemusí být nutně sestavovány v nové přenosové frontě.
4. Volitelné: Monitorování kanálů při přepínání

   V jiném příkazovém okně zobrazte hloubku přenosové fronty během přepínače. Následující příklad zobrazuje stav pro přenosové fronty systémového klastru.

   ```
   DISPLAY QUEUE('SYSTEM.CLUSTER.TRANSMIT.*') CURDEPTH
   ```

5. Volitelné: Monitorujte zprávy AMQ7341 Přenosové fronta pro kanál *ChannelName* přepínané z fronty *QueueName* na *QueueName* , které jsou zapsány do protokolu chyb správce front.

6. Restartujte odesílací kanály klastru, které jste zastavili.

   Kanály se automaticky nespustí, protože jste je zastavili, a převedete je do stavu ZASTAVENO .

```
START CHANNEL(ChannelName)
```

Související odkazy
runswchl
Vyřešit kanál
Ukončit kanál

Klastrování: Doporučené postupy migrace a úprav
Toto téma poskytuje pokyny pro plánování a administraci klastrů IBM MQ . Tyto informace jsou vodítkem na základě testování a zpětné vazby od zákazníků.

1. “Přesouvání objektů v klastru” na stránce 65 (Doporučené postupy pro přesouvání objektů v rámci klastru bez instalace opravných sad nebo nových verzí produktu IBM MQ).
2. “Instalace aktualizací a údržby” na stránce 66 (Doporučené postupy pro udržení funkční architektury klastru v provozu při provádění údržby nebo upgradů a testování nové architektury).

Přesouvání objektů v klastru

Aplikace a jejich fronty

Musíte-li přesunout instanci fronty hostovanou na jednom správci front, aby byla hostována na jiném správci front, můžete pracovat s parametry vyrovnávání pracovní zátěže, abyste zajistili hladký přechod.

Vytvořte instanci fronty, kde má být nově hostována, ale pomocí nastavení vyrovnávání pracovní zátěže klastru pokračujte v odesílání zpráv do původní instance, dokud nebude aplikace připravena k přepnutí. Toho je dosaženo pomocí následujících kroků:

1. Nastavte vlastnost **CLWLRANK** existující fronty na vysokou hodnotu, například pět.
2. Vytvořte novou instanci fronty a nastavte její vlastnost **CLWLRANK** na nulu.
3. Dokončete další konfiguraci nového systému, například implementujte a spusťte spotřebovávající aplikace pro novou instanci fronty.
4. Nastavte vlastnost **CLWLRANK** nové instance fronty na vyšší hodnotu než původní instance, například devět.
5. Povolte původní instanci fronty zpracovat všechny zprávy ve frontě v systému a pak frontu odstraňte.

Přesouvání celých správců front

Pokud správce front zůstává ve stejném hostiteli, ale adresa IP se mění, je proces následující:

- DNS, je-li správně použit, může pomoci zjednodušit proces. Informace o použití DNS nastavením atributu kanálu Název připojení (CONNAME) naleznete v části ALTER CHANNEL.
- Při přesouvání úplného úložiště se před provedením změn ujistěte, že máte alespoň jedno další úplné úložiště, které běží hladce (například bez problémů se stavem kanálu).
- Pozastavte správce front pomocí příkazu SUSPEND QMGR , abyste se vyhnuli nahromadění provozu.
- Upravte adresu IP počítače. Pokud vaše definice kanálu CLUSRCVR používá adresu IP v poli CONNAME, upravte tuto položku adresy IP. Mezipaměť DNS může být nutné vyprázdnit, aby se zajistilo, že aktualizace jsou k dispozici všude.
- Když se správce front znovu připojí k úplným úložištím, automatické definice kanálů se automaticky interpretují.
- Pokud je hostitelem úplného úložiště správce front a změní se adresa IP, je důležité zajistit, aby byly co nejdříve přepnuty části, aby se všechny ručně definované kanály CLUSSDR směrovaly na nové umístění. Až do provedení tohoto přepínače mohou tito správci front kontaktovat pouze zbývající

(nezměněné) úplné úložiště a mohou být zobrazeny varovné zprávy týkající se nesprávné definice kanálu.

- Obnovte činnost správce front pomocí příkazu RESUME QMGR .

Pokud musí být správce front přesunut do nového hostitele, je možné zkopírovat data správce front a obnovit je ze zálohy. Tento proces se však nedoporučuje, pokud nejsou k dispozici žádné další volby; může být lepší vytvořit správce front na novém počítači a replikovat fronty a aplikace, jak je popsáno v předchozí části. Tato situace poskytuje hladký mechanismus přetočení/odvolání.

Pokud jste odhodláni přesunout úplného správce front pomocí zálohy, postupujte podle těchto doporučených postupů:

- Celý proces považujte za obnovu správce front ze zálohy s použitím všech procesů, které byste obvykle používali pro obnovu systému, podle toho, co je vhodné pro vaše prostředí operačního systému.
- Použijte příkaz **REFRESH CLUSTER** po migraci, abyste vyřadili všechny lokálně zadržené informace o klastru (včetně všech automaticky definovaných kanálů, které jsou v nejistém stavu) a vynutili jeho opětovné sestavení.

  Poznámka: U velkých klastrů může být použití příkazu **REFRESH CLUSTER** pro běžící klastr rušivé, a to i nadále vždy každých 27 dnů od tohoto okamžiku, kdy objekty klastru automaticky posílají aktualizace svého stavu na všechny zainteresované správce front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.

Při vytváření správce front a replikaci nastavení z existujícího správce front v klastru (jak bylo popsáno výše v tomto tématu) nikdy nepovažujete dva různé správce front za skutečně stejné. Zejména nezadávejte novému správci front stejný název správce front a adresu IP. Pokus o zrušení náhradního správce front je častou příčinou problémů v klastrech IBM MQ . Mezipaměť očekává přijetí aktualizací včetně atributu **QMID** a stav může být poškozený.

Pokud jsou omylem vytvořeni dva různí správci front se stejným názvem, doporučuje se k vysunutí nesprávné položky z klastru použít příkaz RESET CLUSTER **QMID** .

Instalace aktualizací a údržby

Vyhněte se takzvanému scénáři velkého třesku (například zastavení všech aktivit klastru a správce front, použití všech upgradů a údržby na všechny správce front a následné spuštění všech současně). Klastry jsou navrženy tak, aby stále pracovaly s více verzemi správce front současně, a proto je doporučen dobře plánovaný přístup fázované údržby.

Mít plán zálohování:

- Prováděli jste zálohy?
- Vyvarujte se okamžitého použití nových funkcí klastru: Počkejte, dokud si nebudete jisti, že všichni správci front budou upgradováni na novou úroveň, a ujistěte se, že nebudete odvolávat žádné z nich. Použití nové funkce klastru v klastru, kde jsou někteří správci front stále na dřívější úrovni, může vést k nedefinovanému chování.

  Úložiště ukládá záznam, který obdrží, ve své vlastní verzi. Pokud je záznam, který obdrží, v novější verzi, atributy pozdější verze se vyřadí, když je záznam uložen. Správce front IBM MQ 9.2 přijímající informace o správci front IBM MQ 9.3 ukládá pouze informace IBM MQ 9.2 . Úložiště IBM MQ 9.3 , které přijímá záznam IBM MQ 9.2 , ukládá výchozí hodnoty pro atributy zavedené v novější verzi. Předvolby definují hodnoty pro atributy, které nejsou zahrnuty v záznamu, který přijme.

Nejprve proveďte migraci úplných úložišť. I když mohou předávat informace, kterým nerozumí, nemohou je přetrvat, takže to není doporučený přístup, pokud to není nezbytně nutné. Další informace naleznete v tématu Migrace klastru správce front.

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER
Pomocí příkazu **REFRESH CLUSTER** vyřadíte všechny lokálně uchovávané informace o klastru a znovu sestavíte tyto informace z úplných úložišť v klastru. Tento příkaz byste neměli používat, s výjimkou

výjimečných okolností. Pokud jej potřebujete použít, existují speciální pokyny pro jeho použití. Tyto informace jsou vodítkem na základě testování a zpětné vazby od zákazníků.

Spustit REFRESH CLUSTER pouze v případě, že to opravdu potřebujete

Technologie klastru IBM MQ zajišťuje, že jakákoli změna konfigurace klastru, jako např. změna klastrované fronty, se automaticky stane známou všem členům klastru, kteří potřebují znát informace. K dosažení tohoto šíření informací není třeba dalších administrativních kroků.

Pokud se tyto informace nedostanou ke správcům front v klastru, v němž jsou vyžadovány, například pokud jiný správce front v klastru nezná klastrovanou frontu při prvním pokusu aplikace o její otevření, znamená to problém v infrastruktuře klastru. Je například možné, že nelze spustit kanál mezi správcem front a správcem front úplného úložiště. Proto musí být prozkoumána jakákoli situace, kdy jsou zjištěny nesrovnalosti. Je-li to možné, vyřešte situaci bez použití příkazu **REFRESH CLUSTER** .

Za výjimečných okolností, které jsou zdokumentovány na jiném místě v této dokumentaci produktu, nebo na žádost podpory produktu IBM , můžete použít příkaz **REFRESH CLUSTER** k vyřazení všech lokálně uchovávaných informací o klastru a k opětovnému sestavení těchto informací z úplných úložišť v klastru.

Aktualizace ve velkém klastru může ovlivnit výkon a dostupnost klastru

Použití příkazu **REFRESH CLUSTER** může být v průběhu zpracování klastru s přerušením, například vytvořením náhlého nárůstu práce pro úplná úložiště při zpracování opětovného šíření prostředků klastru správce front. Pokud obnovujete ve velkém klastru (tj. v mnoha stovkách správců front), měli byste se vyhnout použití příkazu v každodenní práci, pokud je to možné, a použít alternativní metody k nápravě specifických nekonzistencí. Není-li například fronta klastru správně šířena v rámci klastru, bude konfigurace fronty v rámci klastru znovu šířena technikou počátečního vyšetřování aktualizace definice klastrované fronty, například změnou jejího popisu. Tento proces může pomoci identifikovat problém a potenciálně vyřešit dočasnou nekonzistenci.

Pokud nelze použít alternativní metody a musíte spustit produkt **REFRESH CLUSTER** ve velkém klastru, měli byste tak učinit v době mimo špičku nebo v okně údržby, abyste se vyhnuli vlivu na pracovní zátěž uživatelů. Měli byste se také vyhnout aktualizaci velkého klastru v jedné dávce a místo toho střídavě rozfázovat aktivitu, jak je vysvětleno v tématu “Vyhněte se problémům s výkonem a dostupností, když objekty klastru odesílají automatické aktualizace” na stránce 67.

Vyhněte se problémům s výkonem a dostupností, když objekty klastru odesílají automatické aktualizace

Po definování nového objektu klastru ve správci front je aktualizace pro tento objekt generována každých 27 dní od okamžiku definice a odeslána do každého úplného úložiště v klastru a dále všem dalším zainteresovaným správcům front. Když zadáte příkaz **REFRESH CLUSTER** pro správce front, resetujete hodiny pro tuto automatickou aktualizaci na všech objektech definovaných lokálně v zadaném klastru.

Pokud aktualizujete velký klastr (tj. mnoho stovek správců front) v jedné dávce nebo za jiných okolností, jako je například opětovné vytvoření systému ze zálohy konfigurace, budou po 27 dnech všichni tito správci front znovu propagovat všechny své definice objektů do úplných úložišť současně. To může znovu způsobit, že systém poběží výrazně pomaleji, nebo se dokonce stane nedostupným, dokud nebudou všechny aktualizace dokončeny. Proto, když musíte aktualizovat nebo znovu vytvořit více správců front ve velkém klastru, měli byste postupně rozfázovat aktivitu na několik hodin nebo několik dní, aby následné automatické aktualizace pravidelně neovlivňovaly výkon systému.

Fronta historie systémového klastru

Po provedení operace **REFRESH CLUSTER** pořídí správce front před aktualizací snímek stavu klastru a uloží jej do úložiště `SYSTEM.CLUSTER.HISTORY.QUEUE` (SCHQ), pokud je definováno ve správci front. Tento snímek je určen pouze pro servisní účely produktu IBM v případě pozdějších problémů se systémem.

SCHQ je při spuštění standardně definován v distribuovaných správcích front. Pro migraci produktu z/OS musí být SCHQ definován ručně.

Platnost zpráv ve výboru SCHQ vyprší po třech měsících.

Související pojmy

“Aspekty příkazu REFRESH CLUSTER pro klastry publikování/odběru” na stránce 102
Po zadání příkazu **REFRESH CLUSTER** bude správce front dočasně vyřazen lokálně uchovávané informace o klastru, včetně všech témat klastru a jejich přidružených proxy odběrů.

Související odkazy

Problémy aplikace při spuštění příkazu REFRESH CLUSTER

Odkaz na příkazy MQSC: REFRESH CLUSTER

Klastrování: Dostupnost, obnova více instancí a zotavení z havárie

Toto téma poskytuje pokyny pro plánování a administraci klastrů IBM MQ . Tyto informace jsou vodítkem na základě testování a zpětné vazby od zákazníků.

IBM MQ Samotné klastrování není řešením vysoké dostupnosti, ale za určitých okolností jej lze použít ke zlepšení dostupnosti služeb pomocí produktu IBM MQ, například tím, že bude mít více instancí fronty v různých správcích front. Tento oddíl poskytuje pokyny k zajištění co nejvyšší dostupnosti infrastruktury IBM MQ , aby ji bylo možné použít v takové architektuře.

Poznámka: Další řešení vysoké dostupnosti a zotavení z havárie jsou k dispozici pro produkt IBM MQ, viz téma Konfigurace vysoké dostupnosti, zotavení a restartování.

Dostupnost prostředků klastru

Obvyklým doporučením pro údržbu dvou úplných úložišť je skutečnost, že ztráta jednoho z nich není kritická pro hladký chod klastru. I když se obojí stane nedostupným, existuje 60denní doba odkladu pro existující znalosti uchovávané dílčími úložišti, ačkoli nové nebo dříve nepřístupné prostředky (například fronty) nejsou v této události k dispozici.

Použití klastrů ke zlepšení dostupnosti aplikací

Klastr může pomoci při návrhu vysoce dostupných aplikací (například serverová aplikace typu požadavek/odezva) pomocí více instancí fronty a aplikace. V případě potřeby mohou atributy priority dávat přednost aktivní aplikaci, pokud například správce front nebo kanál nejsou k dispozici. To je výkonné pro rychlé přepnutí, aby mohlo pokračovat ve zpracování nových zpráv, když dojde k problému.

Zprávy, které byly doručeny konkrétnímu správci front v klastru, jsou však zadrženy pouze v dané instanci fronty a nejsou k dispozici pro zpracování, dokud není tento správce front obnoven. Z tohoto důvodu můžete v případě skutečné vysoké dostupnosti dat zvážit další technologie, například správce front s více instancemi.

Správci front s více instancemi

Software High Availability (multi-instance) je integrovaná nabídka pro zachování dostupnosti vašich stávajících zpráv. Další informace naleznete v tématu Použití produktu IBM MQ s konfiguracemi vysoké dostupnosti, Vytvoření správce front s více instancemia v následující části. Každý správce front v klastru může být pomocí této techniky zpřístupněn s vysokou dostupností, pokud jsou všichni správci front v klastru spuštěni alespoň IBM WebSphere MQ 7.0.1. Pokud se některý správce front v klastru nachází na předchozích úrovních, může dojít ke ztrátě konektivity se správci front s více instancemi v případě, že dojde k překonání selhání na sekundární adresu IP.

Jak již bylo zmíněno v tomto tématu, pokud jsou nakonfigurována dvě úplná úložiště, jsou téměř ze své podstaty vysoce dostupná. V případě potřeby lze pro úplná úložiště použít software IBM MQ High Availability/správce front s více instancemi. Neexistuje žádný silný důvod k použití těchto metod a ve skutečnosti pro dočasné výpadky mohou tyto metody způsobit další náklady na výkon během překonání selhání. Použití vysoké dostupnosti softwaru namísto spuštění dvou úplných úložišť je nevhodné, protože například v případě výpadku jednoho kanálu nemusí nutně dojít k překonání selhání, ale může zanechat částečná úložiště neschopná dotazovat se na prostředky klastru.

Zotavení z havárie

Zotavení z havárie, například zotavení z poškození disků, které ukládají data správce front, je obtížné; produkt IBM MQ může pomoci, ale nemůže to provést automaticky. Jedinou volbou zotavení

z havárie 'true' v produktu IBM MQ (s výjimkou jakéhokoli operačního systému nebo jiných základních replikačních technologií) je obnova ze zálohy. V těchto situacích je třeba zvážit některé specifické body klastru:

- Věnujte pozornost při testování scénářů zotavení z havárie. Pokud například testujete činnost záložních správců front, buďte opatrní při jejich přechodu do režimu online ve stejné síti, protože je možné se náhodně připojit k živému klastru a spustit 'krádež' zpráv hostováním stejných pojmenovaných front jako ve správcích front aktivního klastru.
- Testování zotavení z havárie nesmí kolidovat se spuštěným aktivním klastrem. Techniky, aby se zabránilo rušení patří:
  - Úplné oddělení sítě nebo oddělení na úrovni brány firewall.
  - z/OS Nespouští se inicializace kanálu nebo adresní prostor z/OS **chinit** .
  - Nevydávání aktivního certifikátu TLS do systému pro zotavení z havárie, dokud se neobjeví skutečný scénář zotavení z havárie.
- Při obnově zálohy správce front v klastru je možné, že záloha není synchronizována se zbytkem klastru. Příkaz **REFRESH CLUSTER** může interpretovat aktualizace a synchronizovat s klastrem, ale příkaz **REFRESH CLUSTER** musí být použit jako poslední možnost. Viz “Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 66. Před použitím příkazu zkontrolujte interní dokumentaci procesu a dokumentaci produktu IBM MQ , abyste zjistili, zda nebyl vynechán jednoduchý krok.
- Pokud jde o případnou obnovu, aplikace se musí zabývat přehráváním a ztrátou dat. Je třeba rozhodnout, zda mají být fronty vymazány do známého stavu, nebo zda je k dispozici dostatek informací pro správu opakování.

Plánování distribuované sítě publikování/odběru

Můžete vytvořit síť správců front, v níž budou odběry vytvořené v jednom správci front přijímat odpovídající zprávy publikované aplikací připojenou k jinému správci front v síti. Chcete-li zvolit vhodnou topologii, musíte zvážit své požadavky na ruční řízení, velikost sítě, frekvenci změn, dostupnost a rozšiřitelnost.

Než začnete

Tato úloha předpokládá, že rozumíte tomu, jaké distribuované sítě publikování/odběru jsou a jak fungují. Technický přehled naleznete v tématu Distribuované sítě publikování/odběru.

Informace o této úloze

Existují tři základní topologie pro síť publikování/odběru:

- Klastr s přímým směrovaným spojením
- Klastr směrovaný hostitelem tématu
- Hierarchie

Pro první dvě topologie je výchozím bodem konfigurace klastru IBM MQ . Třetí topologii lze vytvořit s klastrem nebo bez něj. Informace o plánování základní sítě správce front naleznete v části“Plánování distribuovaných front a klastrů” na stránce 19.

Přímo směrovaný klastr je nejjednodušší topologie pro konfiguraci, když je klastr již přítomen. Všechna témata, která definujete v libovolném správci front, jsou automaticky zpřístupněna v každém správci front v klastru a publikování jsou směrována přímo ze všech správců front, v nichž se aplikace publikování připojuje, ke všem správcům front, v nichž existují odpovídající odběry. Tato jednoduchost konfigurace závisí na tom, aby produkt IBM MQ udržoval vysokou úroveň sdílení informací a konektivity mezi jednotlivými správci front v klastru. Pro malé a jednoduché sítě (tj. malý počet správců front a poměrně statická sada vydavatelů a odběratelů) je to přijatelné. Při použití ve větších nebo dynamičtějších prostředích však může být režie nepřípustná. Viz“Přímé směrování v klastrech publikování/odběru” na stránce 74.

Klastr se směrováním hostitelů témat poskytuje stejnou výhodu jako klastr s přímým směrováním, a to tím, že každé téma, které definujete v libovolném správci front v klastru, bude automaticky dostupné v každém správci front v klastru. Klastry se směrováním hostitelů témat však vyžadují, abyste pečlivě vybrali správce front, kteří jsou hostiteli jednotlivých témat, protože všechny informace a publikace pro dané téma procházejí těmito správci front hostitele témat. To znamená, že systém nemusí udržovat kanály a informační toky mezi všemi správci front. To však také znamená, že publikování již nemusí být odesílána přímo odběratelům, ale mohou být směrována prostřednictvím správce front hostitele tématu. Z těchto důvodů může být do systému vloženo další zatížení, zejména do správců front, kteří jsou hostitelem témat, takže je nutné pečlivé plánování topologie. Tato topologie je zvláště účinná pro sítě, které obsahují mnoho správců front nebo jsou hostiteli dynamické sady vydavatelů a odběratelů (tj. vydavatelů nebo odběratelů, kteří jsou často přidáváni nebo odebíráni). Další hostitele témat lze definovat za účelem zlepšení dostupnosti tras a horizontálního měřítka pracovní zátěže publikování. Viz"Směrování hostitelů témat v klastrech publikování/odběru" na stránce 79.

Hierarchie vyžaduje, aby byla nastavena nejvíce ruční konfigurace, a jedná se o nejtěžší topologii, kterou lze upravit. Vztahy mezi jednotlivými správci front v hierarchii a jejich přímé vztahy je třeba konfigurovat ručně. Po konfiguraci vztahů budou publikování (stejně jako v předchozích dvou topologiích) směrována na odběry jiných správců front v hierarchii. Publikování jsou směrována pomocí hierarchických vztahů. To umožňuje konfigurovat velmi specifické topologie tak, aby vyhovovaly různým požadavkům, ale může to také vést k publikování, která vyžadují mnoho "přechodů" prostřednictvím intermediačních správců front pro dosažení odběrů. Existuje vždy pouze jedna trasa přes hierarchii pro publikování, takže dostupnost každého správce front je kritická. Hierarchie jsou obvykle vhodné pouze v případech, kdy jeden klastr nelze konfigurovat; například při překlenutí více organizací. Viz"Směrování v hierarchiích publikování/odběru" na stránce 102.

V případě potřeby lze výše uvedené tři topologie kombinovat, aby se vyřešily specifické topografické požadavky. Příklad viz Kombinace prostorů témat více klastrů.

Chcete-li zvolit vhodnou topologii pro vaši distribuovanou síť publikování/odběru, musíte zvážit následující široké otázky:

- Jak velká bude vaše síť?
- Kolik ruční kontroly potřebujete nad jeho konfigurací?
- Jak bude systém dynamický, a to jak z hlediska témat a odběrů, tak z hlediska správců front?
- Jaké jsou vaše požadavky na dostupnost a rozšiřitelnost?
- Mohou se všichni správci front připojovat přímo k sobě?

Procedura

- Odhadněte, jak velká musí být vaše síť.
  a) Odhadněte, kolik témat potřebujete.
  b) Odhadněte, kolik vydavatelů a odběratelů očekáváte.
  c) Odhadněte, kolik správců front bude zapojeno do aktivit publikování/odběru.

     Viz také"Klastrování publikování/odběru: Doporučené postupy" na stránce 88, zejména následující sekce:

     – Jak upravit velikost systému
     – Důvody pro omezení počtu správců front klastru zapojených do aktivity publikování/odběru
     – Jak rozhodnout, která témata se mají klastrovat

  Pokud bude mít vaše síť mnoho správců front a bude pracovat s mnoha vydavateli a odběrateli, budete pravděpodobně muset použít klastr nebo hierarchii se směrovaným hostitelem tématu. Přímo směrované klastry nevyžadují téměř žádnou ruční konfiguraci a mohou být dobrým řešením pro malé nebo statické sítě.
- Zvažte, kolik ruční kontroly potřebujete nad tím, který správce front je hostitelem jednotlivých témat, vydavatelů nebo odběratelů.

a) Zvažte, zda jsou někteří z vašich správců front méně schopní než jiní.

b) Zvažte, zda jsou komunikační odkazy na některé z vašich správců front křehčí než na jiné.

c) Identifikujte případy, kdy očekáváte, že téma bude mít mnoho publikací a málo odběratelů.

d) Identifikujte případy, kdy očekáváte, že téma bude mít mnoho odběratelů a několik publikací.

Ve všech topologiích jsou publikování doručována odběrům v jiných správcích front. V přímo směrovaném klastru se tato publikování nacházejí v nejkratší cestě k odběrům. V klastru nebo hierarchii směrovaných hostitelů témat řídíte trasu, kterou mají publikování. Pokud se vaši správci front liší svými schopnostmi nebo mají různé úrovně dostupnosti a konektivity, budete pravděpodobně chtít přiřadit specifické pracovní zátěže specifickým správcům front. To lze provést buď pomocí klastru se směrovaným hostitelem tématu, nebo pomocí hierarchie.

Ve všech topologiích společné umístění publikačních aplikací ve stejném správci front jako odběry, kdykoli je to možné, minimalizuje režijní náklady a maximalizuje výkon. V případě klastrů směrovaných hostiteli témat zvažte umístění vydavatelů nebo odběratelů do správců front, kteří jsou hostiteli tématu. Dojde k odebrání všech dalších "přechodů" mezi správci front pro předání publikování odběrateli. Tento přístup je zvláště účinný v případech, kdy téma má mnoho vydavatelů a málo odběratelů, nebo mnoho odběratelů a málo vydavatelů. Viz například Směrování hostitelů témat pomocí centralizovaných vydavatelů nebo odběratelů.

Viz také“Klastrování publikování/odběru: Doporučené postupy” na stránce 88, zejména následující sekce:

– Jak rozhodnout, která témata se mají klastrovat
– Umístění vydavatele a odběru

- Zvažte, jak dynamická bude síťová aktivita.

  a) Odhadněte, jak často budou odběratelé přidáváni a odebíráni k různým tématům.

  Kdykoli je odběr přidán nebo odebrán ze správce front a jedná se o první nebo poslední odběr daného řetězce tématu, jsou tyto informace sdělovány ostatním správcům front v topologii. V přímo směrovaném klastru a hierarchii jsou tyto informace o odběru šířeny do všech správců front v topologii bez ohledu na to, zda mají v tématu vydavatele. Pokud se topologie skládá z mnoha správců front, může se jednat o významnou režii výkonu. V klastru se směrovaným hostitelem tématu jsou tyto informace šířeny pouze do správců front, kteří jsou hostiteli klastrovaného tématu mapovaného na řetězec tématu odběru.

  Viz také část Změna odběru a dynamické řetězce témat v části“Klastrování publikování/odběru: Doporučené postupy” na stránce 88.

  Poznámka: Ve velmi dynamických systémech, kde se sada mnoha jedinečných řetězců témat rychle a neustále mění, může být nejlepší přepnout model do režimu "publikovat všude" . Viz Výkon odběru v sítích publikování/odběru.

  b) Zvažte, jak jsou dynamičtí správci front v topologii.

  Hierarchie vyžaduje, aby každá změna ve správci front v topologii byla ručně vložena nebo odebrána z hierarchie, s opatrností při změně správců front na vyšších úrovních v hierarchii. Správci front v hierarchii obvykle používají také ručně konfigurovaná připojení kanálu. Tato připojení je nutné udržovat, přidávat a odebírat kanály jako správce front a odebírat je z hierarchie.

  V klastru publikování/odběru jsou správci front automaticky připojeni k libovolnému jinému správci front, který je vyžadován při prvním připojení ke klastru, a automaticky se dozví o tématech a odběrech.

- Zvažte dostupnost trasy a požadavky na rozšiřitelnost publikačního provozu.

  a) Rozhodněte, zda potřebujete mít vždy k dispozici trasu ze správce front publikování do správce front odběru, a to i v případě, že správce front není k dispozici.

  b) Zamyslete se nad tím, jak rozšiřitelnou síť potřebujete. Rozhodněte, zda je úroveň publikačního provozu příliš vysoká na to, aby mohla být směrována prostřednictvím jednoho správce front nebo kanálu, a zda musí být tato úroveň publikačního provozu zpracována jednou větví tématu nebo zda ji lze rozdělit mezi více větví tématu.

c) Zvažte, zda je třeba udržovat pořadí zpráv.

Vzhledem k tomu, že klastr s přímým směrováním odesílá zprávy přímo ze správců front publikování odebírajícím správcům front, není nutné brát v úvahu dostupnost intermediačních správců front na trase. Stejně tak není třeba brát v úvahu škálování na intermediační správce front. Jak již bylo zmíněno, režie automatické správy kanálů a informačních toků mezi všemi správci front v klastru může významně ovlivnit výkon, zejména ve velkém nebo dynamickém prostředí.

Klastr směrovaný hostitelem tématu lze vyladit pro jednotlivá témata. Můžete zajistit, aby každá větev stromu témat, která má značnou pracovní zátěž publikování, byla definována v jiném správci front a aby byl každý správce front dostatečně výkonný a dostupný pro očekávanou pracovní zátěž pro danou větev stromu témat. Dále můžete zlepšit dostupnost a vodorovné škálování definováním jednotlivých témat ve více správcích front. To umožňuje systému směrovat nedostupné správce front hostitele tématu a vyrovnávat pracovní zátěž publikačních přenosů v rámci těchto správců. Definujete-li však dané téma ve více správcích front, zavedete také následující omezení:

– Ztratíte řazení zpráv napříč publikacemi.
– Zachovaná publikování nelze použít. Viz“Aspekty návrhu pro zachovaná publikování v klastrech publikování/odběru” na stránce 100.

Nelze konfigurovat vysokou dostupnost nebo rozšiřitelnost směrování v hierarchii prostřednictvím více přenosových cest.

Viz také část Provoz publikování v části“Klastrování publikování/odběru: Doporučené postupy” na stránce 88.

- Na základě těchto výpočtů použijte poskytnuté odkazy, které vám pomohou rozhodnout, zda použít klastr hostitele se směrovaným tématem, klastr s přímým směrovaným směrem, hierarchii nebo kombinaci těchto topologií.

Jak pokračovat dále

Nyní jste připraveni nakonfigurovat distribuovanou síť publikování/odběru.

Související úlohy

Konfigurace klastru správců front

Konfigurace distribuovaných front

Konfigurace klastru publikování/odběru

Připojení správce front k hierarchii publikování/odběru

Návrh klastrů publikování/odběru

Existují dvě základní topologie klastru publikování/odběru: *přímé směrování* a *směrování hostitele tématu*. Každý z nich má jiné výhody. Při návrhu klastru publikování/odběru zvolte topologii, která nejlépe vyhovuje vašim očekávaným síťovým požadavkům.

Přehled dvou topologií klastru publikování/odběru viz Klastry publikování/odběru. Informace, které vám pomohou vyhodnotit požadavky na síť, naleznete v části “Plánování distribuované sítě publikování/odběru” na stránce 69 a “Klastrování publikování/odběru: Doporučené postupy” na stránce 88.

Obecně platí, že obě topologie klastru poskytují následující výhody:

- Jednoduchá konfigurace nad topologií dvoubodového klastru.
- Automatické zpracování správců front, kteří se připojují ke klastru a opouštějí jej.
- Snadné škálování pro další odběry a vydavatele, a to přidáním dalších správců front a distribucí dalších odběrů a vydavatelů napříč nimi.

Avšak tyto dvě topologie mají různé výhody, protože požadavky se stávají konkrétnějšími.

Přímo směrované klastry publikování/odběru

V případě přímého směrování odesílá každý správce front v klastru publikování z připojených aplikací přímo všem ostatním správcům front v klastru s odpovídajícím odběrem.

Přímý klastr publikování/odběru poskytuje následující výhody:

- Zprávy určené pro odběr ve specifickém správci front ve stejném klastru jsou přenášeny přímo do tohoto správce front a nemusí procházet prostředním správcem front. To může zlepšit výkon v porovnání s topologií směrovanou hostitelem tématu nebo hierarchickou topologií.
- Vzhledem k tomu, že všichni správci front jsou navzájem přímo připojeni, neexistuje jediný bod selhání v infrastruktuře směrování této topologie. Pokud jeden správce front není k dispozici, mohou odběry v jiných správcích front v klastru i nadále přijímat zprávy od vydavatelů v dostupných správcích front.
- Konfigurace je velmi jednoduchá, zejména na existujícím klastru.

Věci, které je třeba zvážit při použití klastru přímého směrovaného publikování/odběru:

- Všichni správci front v klastru budou informováni o všech ostatních správcích front v klastru.
- Správci front v klastru, který je hostitelem jednoho či více odběrů klastrovaného tématu, automaticky vytvoří odesílací kanály klastru pro všechny ostatní správce front v klastru, a to i v případě, že tito správci front nepublikují zprávy v klastrovaných tématech.
- První odběr řetězce tématu ve správci front v rámci klastrovaného tématu má za následek odeslání zprávy všem ostatním správcům front v klastru. Podobně i poslední odběr v řetězci tématu, který má být odstraněn, má za následek zprávu. Čím více jednotlivých řetězců témat je používáno v rámci klastrovaného tématu a čím vyšší je četnost změn odběrů, tím více dochází ke komunikaci mezi správci front.
- Každý správce front v klastru uchovává informace o odebíraných řetězcích témat, o nichž je informován, a to i v případě, že správce front tato témata nepublikuje ani neodebírá.

Z výše uvedených důvodů budou mít všichni správci front v klastru s definovaným tématem s přímým směrováním další režii. Čím více správců front je v klastru, tím větší režie. Podobně platí, že čím více řetězců témat se přihlásí k odběru, a tím větší je jejich rychlost změn, tím větší je režie. To může vést k příliš velkému zatížení správců front spuštěných v malých systémech ve velkém nebo dynamickém klastru pro přímé publikování/odběr. Další informace viz Výkon přímého směrovaného publikování/odběru .

Když víte, že klastr nemůže pojmout režijní náklady přímo směrovaného klastrovaného publikování/odběru, můžete místo toho použít hostitel tématu směrovaný publikování/odběr. V extrémních situacích můžete funkci klastrovaného publikování/odběru zcela zakázat nastavením atributu správce front **PSCLUS** na hodnotu DISABLED v každém správci front v klastru. Viz “Blokování klastrovaného publikování/odběru” na stránce 98. Tím zabráníte vytvoření jakéhokoli klastrovaného tématu, a zajistíte tak, že vaše síť nebude nést žádné režijní náklady přidružené k klastrovanému publikování/odběru.

Klastry publikování/odběru se směrovaným hostitelem tématu

V případě směrování hostitelů témat se správci front, v nichž jsou administrativně definována klastrovaná témata, stanou směrovači pro publikování. Publikace od nehostitelských správců front v klastru jsou směrovány prostřednictvím hostitelského správce front do libovolného správce front v klastru s odpovídajícím odběrem.

Klastr publikování/odběru se směrovaným hostitelem tématu poskytuje následující další výhody oproti klastru přímého směrovaného publikování/odběru:

- O všech ostatních správcích front v klastru jsou informováni pouze správci front, pro které jsou definována témata směrovaná hostitelem tématu.
- Pouze správci front hostitele tématu musí být schopni se připojit ke všem ostatním správcům front v klastru a obvykle se budou připojovat pouze k těm, kde existují odběry. Proto je mezi správci front spuštěno výrazně méně kanálů.
- Správci front klastru, kteří jsou hostiteli jednoho nebo více odběrů klastrovaného tématu, automaticky vytvoří odesílací kanály klastru pouze pro správce front, kteří jsou hostiteli tématu klastru mapovaného na řetězec tématu odběru.
- První odběr řetězce tématu ve správci front v rámci klastrovaného tématu má za následek odeslání zprávy správci front v klastru, který je hostitelem klastrovaného tématu. Podobně i poslední odběr

v řetězci tématu, který má být odstraněn, má za následek zprávu. Čím více jednotlivých řetězců témat používaných v rámci klastrovaného tématu a čím vyšší je četnost změn odběrů, tím více dochází ke komunikaci mezi správci front, ale pouze mezi hostiteli odběrů a hostiteli témat.

- Větší kontrola nad fyzickou konfigurací. S přímým směrováním se musí všichni správci front účastnit klastru publikování/odběru, což zvýší jejich režijní náklady. Při směrování hostitelů témat jsou o ostatních správcích front a jejich odběrech informováni pouze správci front hostitele témat. Explicitně vyberete správce front hostitele tématu, takže můžete zajistit, aby tito správci front byli spuštěni na odpovídajícím vybavení, a pro ostatní správce front můžete používat méně výkonné systémy.

Věci, které je třeba zvážit při použití klastru publikování/odběru se směrovaným hostitelem tématu:

- Další "přechod" mezi správcem front publikování a správcem front odběru je zaveden v případě, že vydavatel nebo odběratel není umístěn v tématu, které je hostitelem správce front. Latence způsobená nadbytečným "přechodem" může znamenat, že směrování hostitele tématu je méně efektivní než přímé směrování.
- Na velkých klastrech usnadňuje směrování hostitelů témat významný výkon a škálování problémů, které můžete získat s přímým směrováním.
- Můžete se rozhodnout definovat všechna témata pro jednoho správce front nebo pro velmi malý počet správců front. Pokud tak učiníte, ujistěte se, že správci front hostitele tématu jsou hostováni na výkonných systémech s dobrou konektivitou.
- Stejné téma můžete definovat ve více než jednom správci front. To zlepšuje dostupnost tématu a také zvyšuje rozšiřitelnost, protože IBM MQ vyrovnává pracovní zátěž publikování pro téma ve všech hostitelích daného tématu. Mějte však na paměti, že definování stejného tématu ve více než jednom správci front ztratí pořadí zpráv pro toto téma.
- Díky hostování různých témat v různých správcích front můžete zlepšit rozšiřitelnost bez ztráty pořadí zpráv.

Související úlohy

Scénář: Vytvoření klastru publikování/odběru

Konfigurace klastru publikování/odběru

Vyladění distribuovaných sítí publikování/odběru

Odstraňování problémů s distribuovaným publikováním/odběry

Přímé směrování v klastrech publikování/odběru

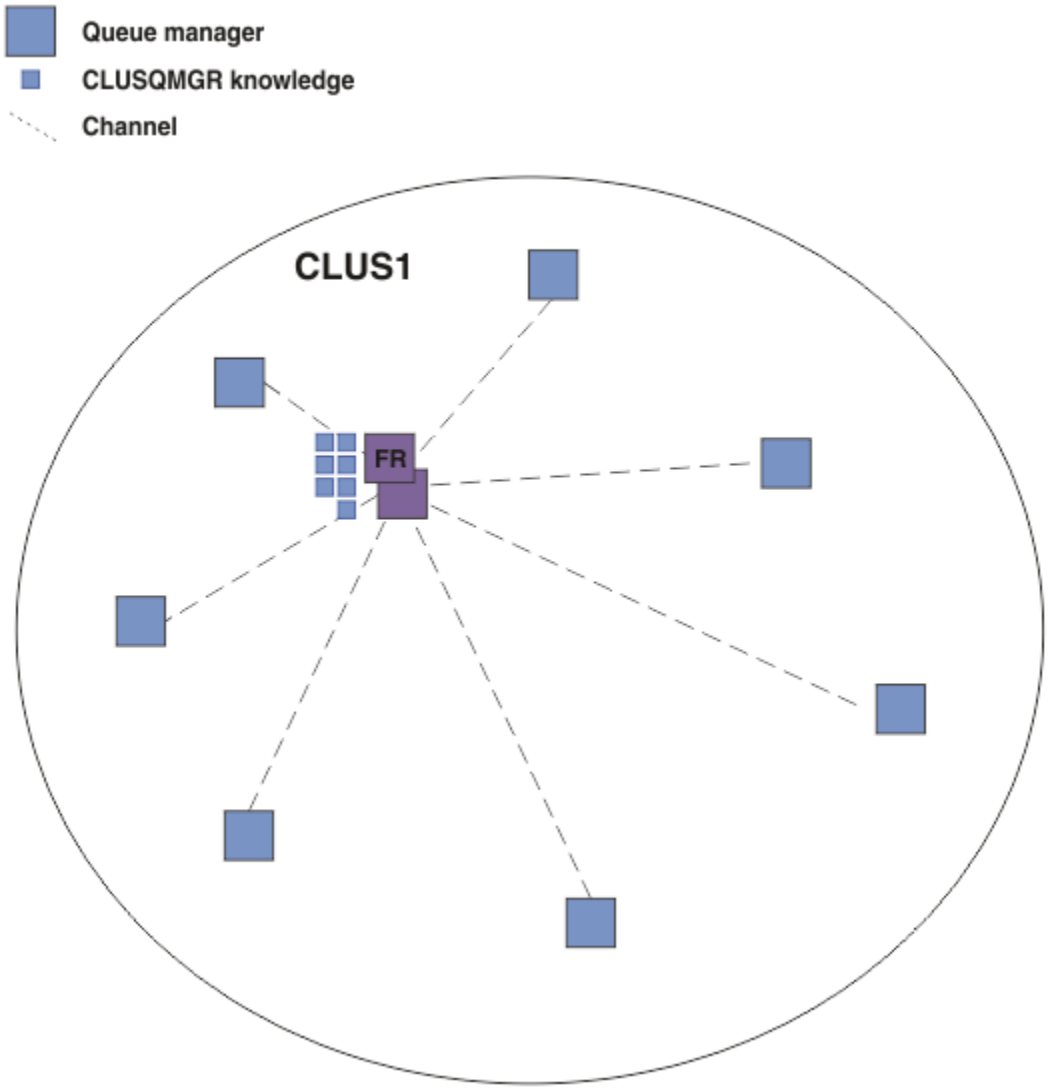
Publikace z libovolného správce front publikování jsou směrovány přímo na jiného správce front v klastru s odpovídajícím odběrem.

Úvodní informace o směrování zpráv mezi správci front v hierarchiích publikování/odběru a v klastrech naleznete v tématu Distribuované sítě publikování/odběru.

Klastr publikování/odběru s přímým směrovaným názvem se chová takto:

- Všichni správci front automaticky znají všechny ostatní správce front.
- Všichni správci front s odběry klastrovaných témat vytvářejí kanály pro všechny ostatní správce front v klastru a informují je o svých odběrech.
- Zprávy publikované aplikací jsou směrovány ze správce front, ke kterému je připojena, přímo na každého správce front, kde existuje odpovídající odběr.

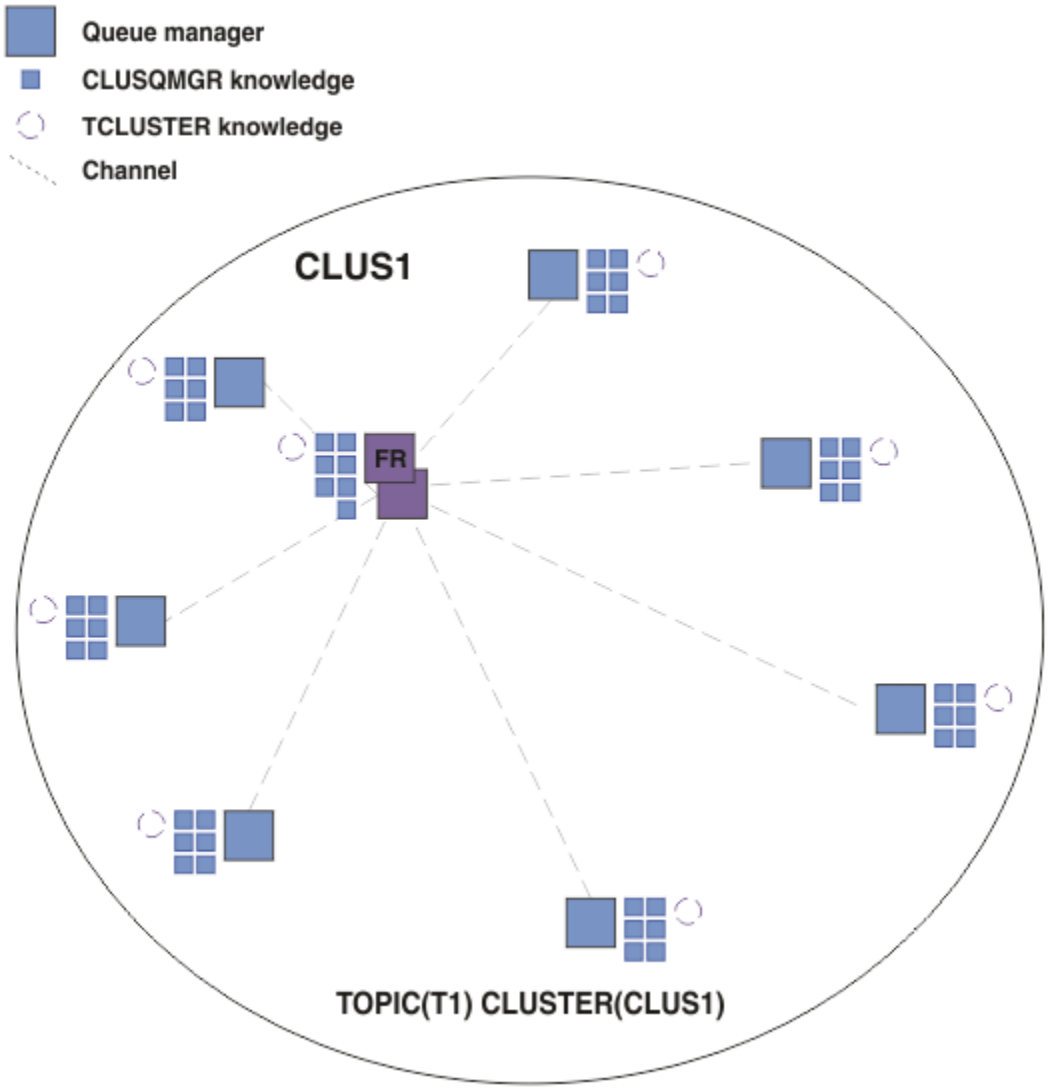
Následující diagram zobrazuje klastr správců front, který se aktuálně nepoužívá pro aktivity publikování/odběru nebo dvoubodové aktivity. Uvědomte si, že každý správce front v klastru se připojuje pouze ke správcům front úplného úložiště a z nich.



Obrázek 16. Klastr správců front

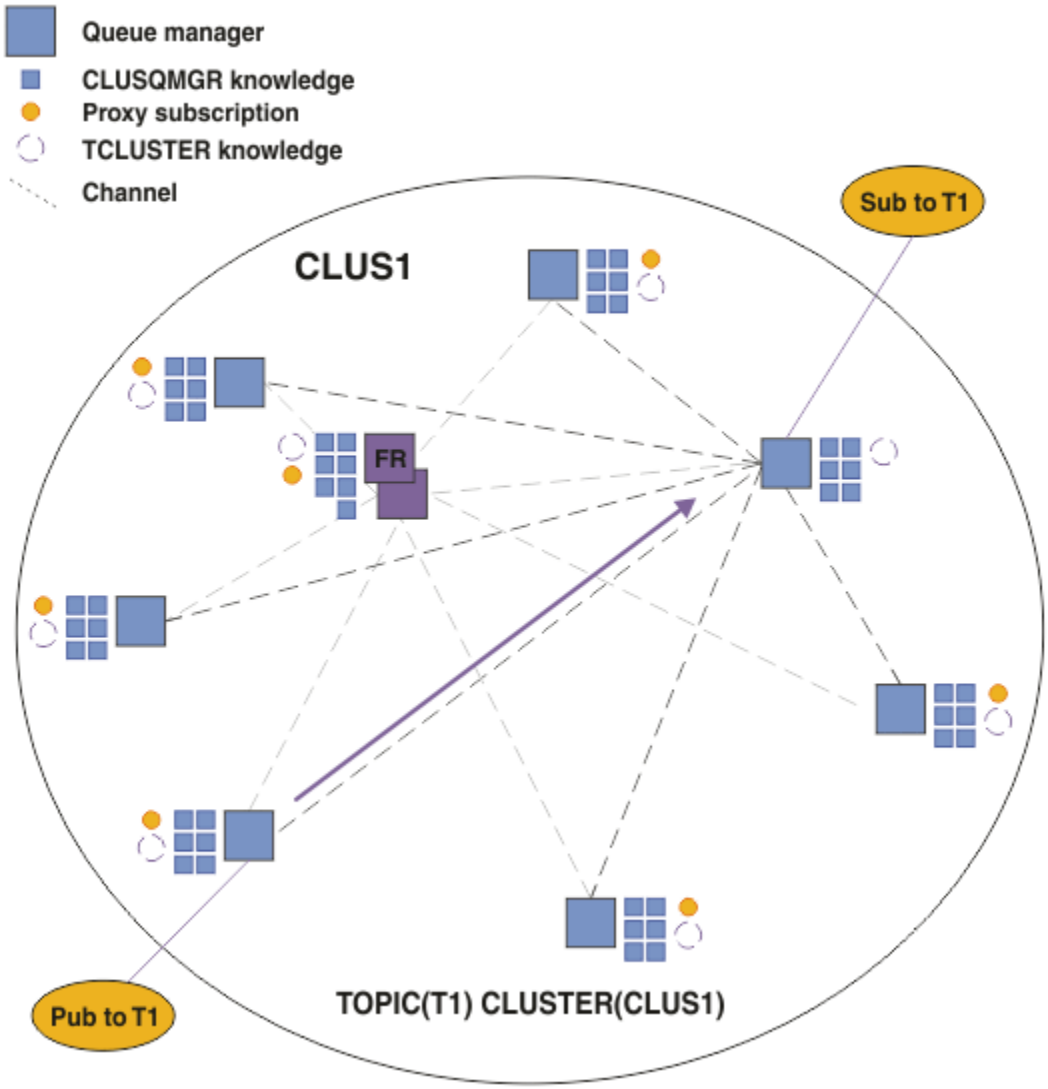
V případě publikování, která mají proudit mezi správci front v klastru s přímým směrováním, můžete vytvořit klastr pro větev stromu témat, jak je popsáno v tématu Konfigurace klastru publikování/odběru, a určit *přímé směrování* (výchozí nastavení).

V přímo směrovaném klastru publikování/odběru definujete objekt tématu v libovolném správci front v klastru. Pokud tak učiníte, znalost objektu a znalost všech ostatních správců front v klastru budou správci front s úplným úložištěm automaticky přesunuty do všech správců front v klastru. K tomu dochází před tím, než některý správce front odkazuje na téma:



Obrázek 17. Přímo směrovaný klastr publikování/odběru

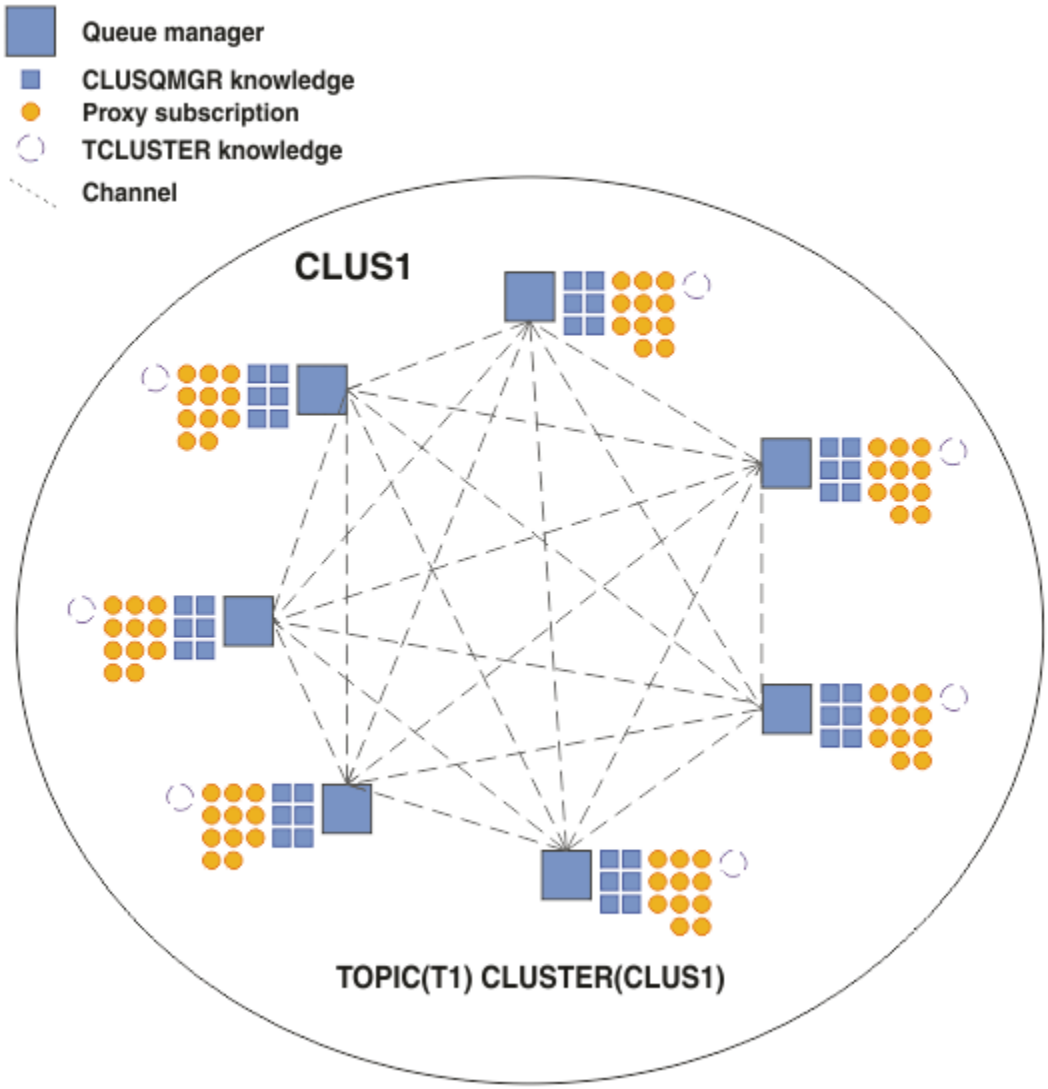
Při vytvoření odběru vytvoří správce front, který je hostitelem odběru, kanál pro každého správce front v klastru a odešle podrobnosti o odběru. Tyto znalosti distribuovaného odběru jsou reprezentovány proxy odběrem v jednotlivých správcích front. Při vytváření publikování v libovolném správci front v klastru, který odpovídá řetězci tématu daného odběru proxy, se vytvoří kanál klastru od správce front vydavatele ke každému správci front, který je hostitelem odběru, a zpráva se odešle každému z nich.



Obrázek 18. Přímo směrovaný klastr publikování/odběru s vydavatelem a odběratelem klastrovaného tématu.

Přímé směrování publikování na správce front hostující odběr zjednodušuje konfiguraci a minimalizuje latenci při doručování publikací k odběrům.

V závislosti na umístění odběrů a vydavatelů se však může klastr rychle stát plně propojeným, přičemž každý správce front má přímé připojení ke všem ostatním správcům front. To může nebo nemusí být přijatelné ve vašem prostředí. Podobně platí, že pokud se často mění sada řetězců témat, k jejichž odběru se odebírají, může se také výrazná režie šíření těchto informací mezi všemi správci front. Všichni správci front v přímo směrovaném klastru publikování/odběru musí být schopni se s těmito režijními náklady vyrovnat.



Obrázek 19. Klastr s přímým směrovaným publikování/odběrem, který je plně propojený

Souhrn a další aspekty

Klastr s přímým směrováním publikování/odběru vyžaduje malý ruční zásah pro vytvoření nebo správu a poskytuje přímé směrování mezi vydavateli a odběrateli. Pro určité konfigurace se obvykle jedná o nejvhodnější topologii, zejména klastry s malým počtem správců front, nebo kde je přijatelná vysoká konektivita správců front a odběry se mění zřídka. Nicméně to také ukládá určitá omezení na vašem systému:

- Zátěž každého správce front je úměrná celkovému počtu správců front v klastru. Proto se ve větších klastrech mohou jednotliví správci front a systém jako celek setkat s problémy s výkonem.
- Při výchozím nastavení jsou všechny řetězce klastrovaných témat, které jsou přihlášeny k odběru, šířeny v rámci klastru a publikování jsou šířena pouze do vzdálených správců front, kteří mají odběr přidruženého tématu. Proto se rychlé změny v sadě odběrů mohou stát limitujícím faktorem. Toto výchozí chování můžete změnit a místo toho můžete všechna publikování šířit do všech správců front, což odebere potřebu proxy odběrů. Tím se snižuje přenos znalostí odběru, ale je pravděpodobné, že se zvýší provoz publikování a počet kanálů, které každý správce front zavede. Viz Výkon odběru v sítích publikování/odběru.

  Poznámka: Podobné omezení platí i pro hierarchie.

- Vzhledem k vzájemně provázané povaze správců front publikování/odběru trvá, než se proxy odběry rozšíří kolem všech uzlů v síti. Vzdálená publikování nemusí být nutně okamžitě přihlášena k odběru, takže po přihlášení k odběru nového řetězce tématu nemusí být odeslána časná publikování. Problémy způsobené prodlevou odběru můžete odebrat tak, že všechny publikace budou šířeny do všech správců front, což odstraní potřebu proxy odběrů. Viz Výkon odběru v sítích publikování/odběru.

  Poznámka: Toto omezení platí také pro hierarchie.

Před použitím přímého směrování prozkoumejte alternativní přístupy popsané v části “Směrování hostitelů témat v klastrech publikování/odběru” na stránce 79a “Směrování v hierarchiích publikování/odběru” na stránce 102.

Směrování hostitelů témat v klastrech publikování/odběru

Publikace od nehostitelských správců front v klastru jsou směrovány prostřednictvím hostitelského správce front do libovolného správce front v klastru s odpovídajícím odběrem.

Úvodní informace o směrování zpráv mezi správci front v hierarchiích publikování/odběru a v klastrech naleznete v tématu Distribuované sítě publikování/odběru.

Chcete-li porozumět chování a výhodám směrování hostitelů témat, je nejlepší nejprve porozumět “Přímé směrování v klastrech publikování/odběru” na stránce 74.

Klastr publikování/odběru směrovaný hostitelem tématu se chová takto:

- Objekty klastrovaných spravovaných témat jsou ručně definovány v jednotlivých správcích front v klastru. Tyto položky jsou označovány jako *správci front hostitele tématu*.
- Při vytváření odběru pro správce front klastru jsou vytvořeny kanály ze správce front hostitele odběru pro správce front hostitele tématu a proxy odběry jsou vytvořeny pouze pro správce front, kteří jsou hostiteli tématu.
- Když aplikace publikuje informace do tématu, připojený správce front vždy předá publikování jednomu správci front, který je hostitelem tématu, a předá je všem správcům front v klastru, kteří mají odpovídající odběry pro dané téma.

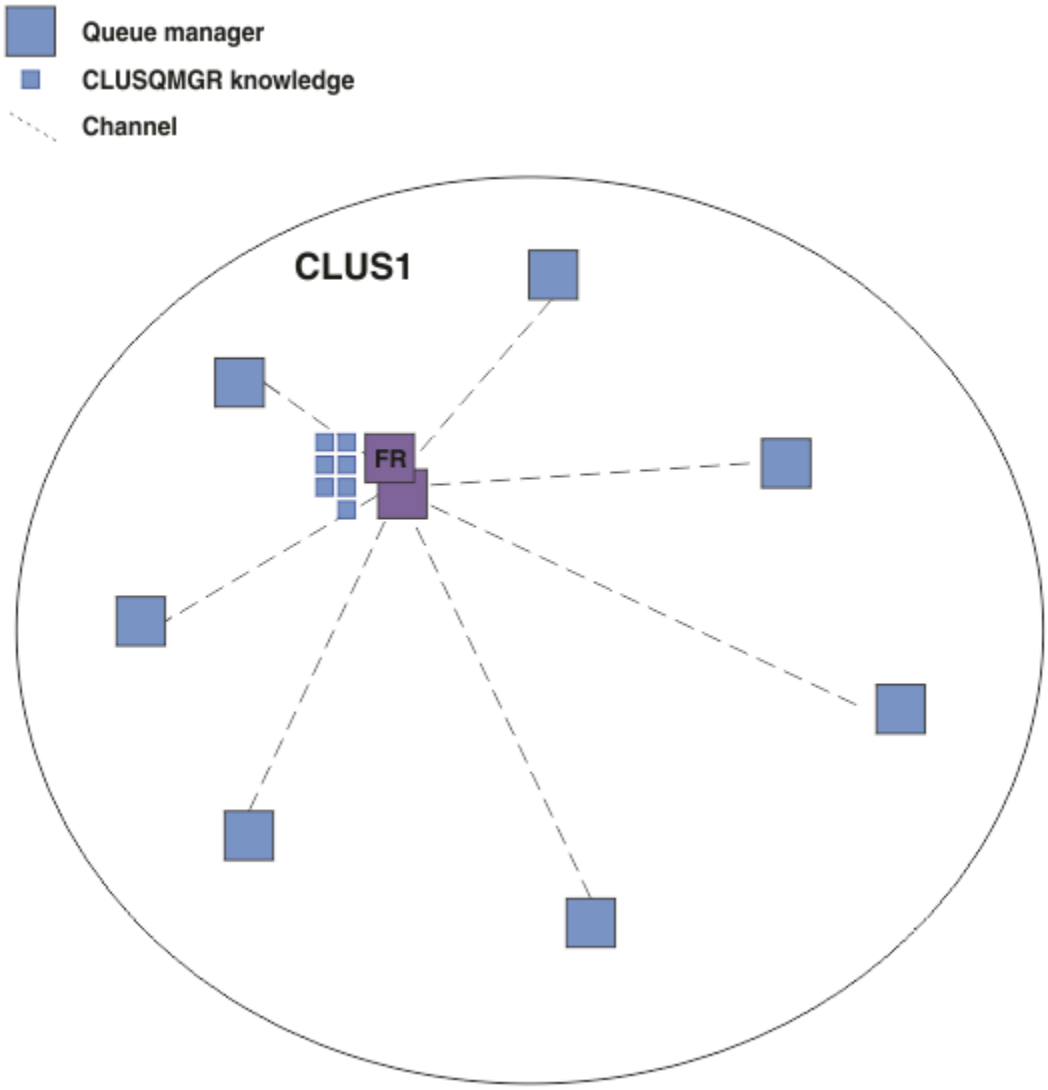
Tento proces je podrobněji vysvětlen v následujících příkladech.

Směrování hostitele tématu pomocí jednoho hostitele tématu

V případě publikování pro tok mezi správci front v klastru se směrováním hostitele tématu vytvoříte klastr větve stromu témat, jak je popsáno v tématu Konfigurace klastru publikování/odběru, a určíte *směrování hostitele tématu*.

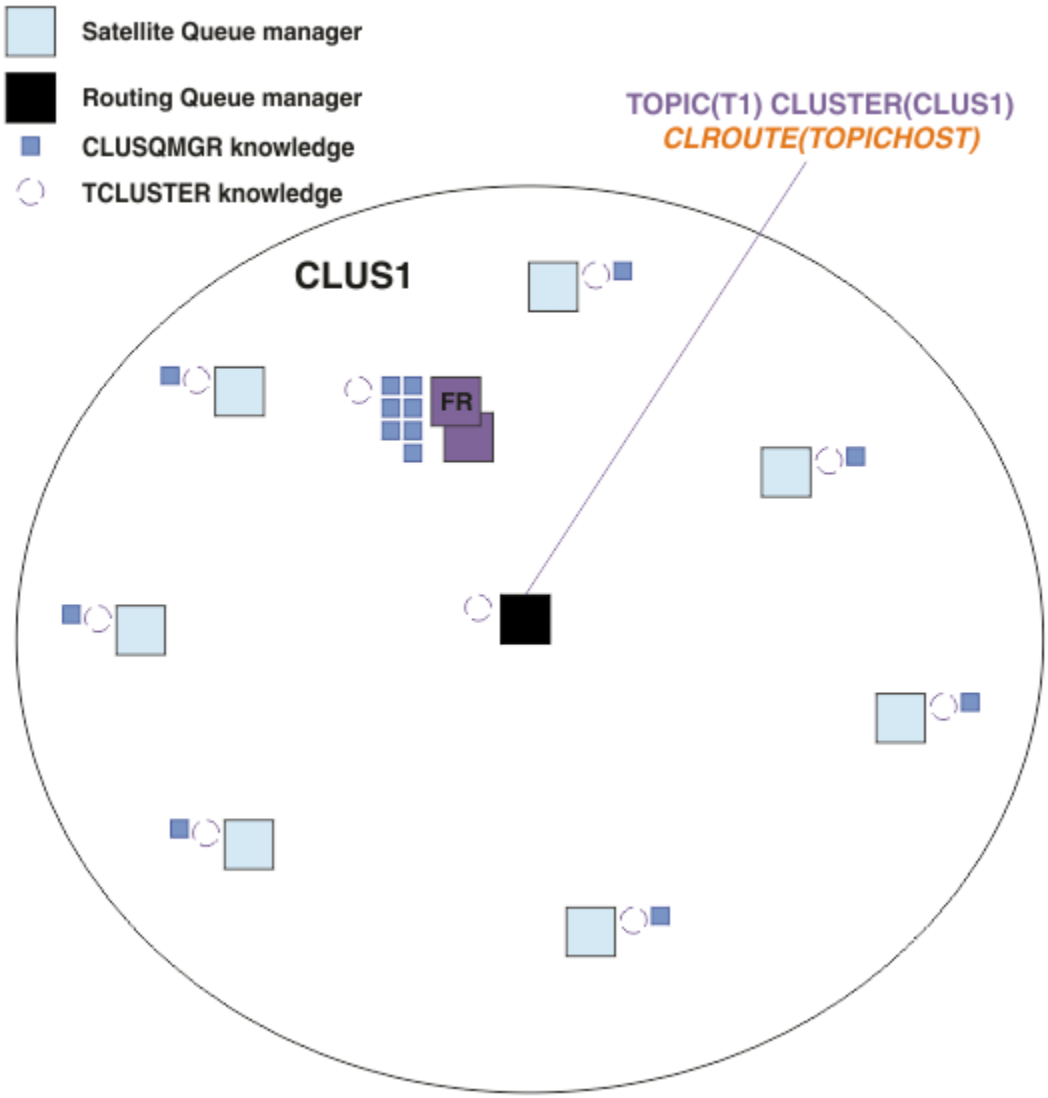
Existuje řada příčin pro definování objektu tématu směrovaného hostitelem tématu ve více správcích front v klastru. Nicméně, pro jednoduchost začneme s jedním tématem hostitele.

Následující diagram zobrazuje klastr správců front, který se aktuálně nepoužívá pro aktivity publikování/odběru nebo dvoubodové aktivity. Uvědomte si, že každý správce front v klastru se připojuje pouze ke správcům front úplného úložiště a z nich.



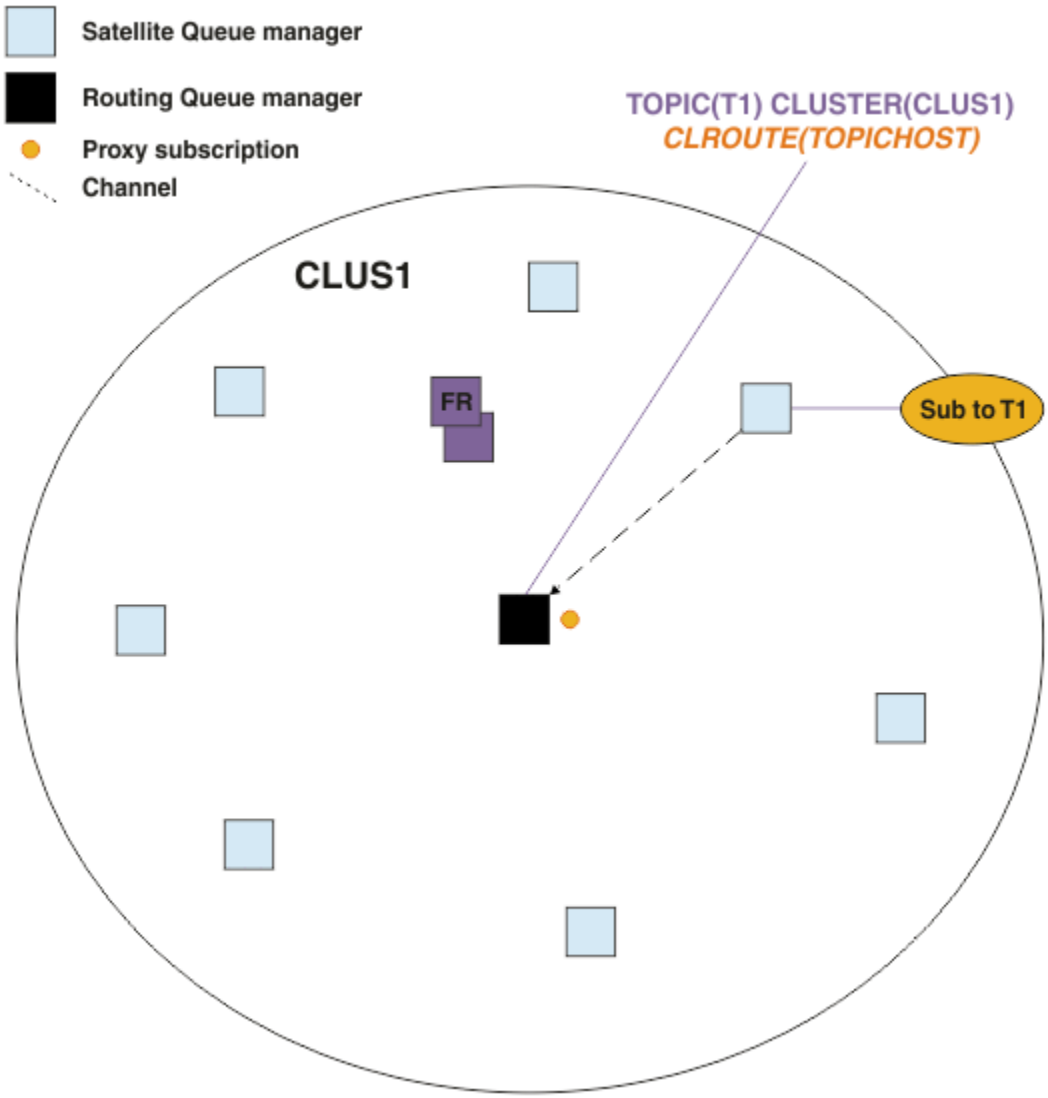
Obrázek 20. Klastr správců front

V klastru publikování/odběru směrovaném hostitelem tématu definujete objekt tématu ve specifickém správci front v klastru. Provoz publikování/odběru poté prochází tímto správcem front, což z něj činí kritického správce front v klastru a zvyšuje jeho pracovní zátěž. Z těchto důvodů se nedoporučuje používat správce front úplného úložiště, ale jiného správce front v klastru. Definujete-li objekt tématu ve správci front hostitele, budou informace o objektu a jeho hostiteli automaticky odeslány správci front úplného úložiště všem ostatním správcům front v klastru. Všimněte si, že na rozdíl od *přímého směrování*není každému správci front sděleno o každém jiném správci front v klastru.



Obrázek 21. Klastr publikování/odběru směrovaný hostitelem tématu s jedním tématem definovaným na jednom hostiteli tématu.

Při vytvoření odběru ve správci front je vytvořen kanál mezi odebírajícím správcem front a správcem front hostitele tématu. Odebírající správce front se připojí pouze ke správci front hostitele tématu a odešle podrobnosti o odběru (ve formě *proxy odběru*). Správce front hostitele tématu nepředává tyto informace o odběru dalším správcům front v klastru.

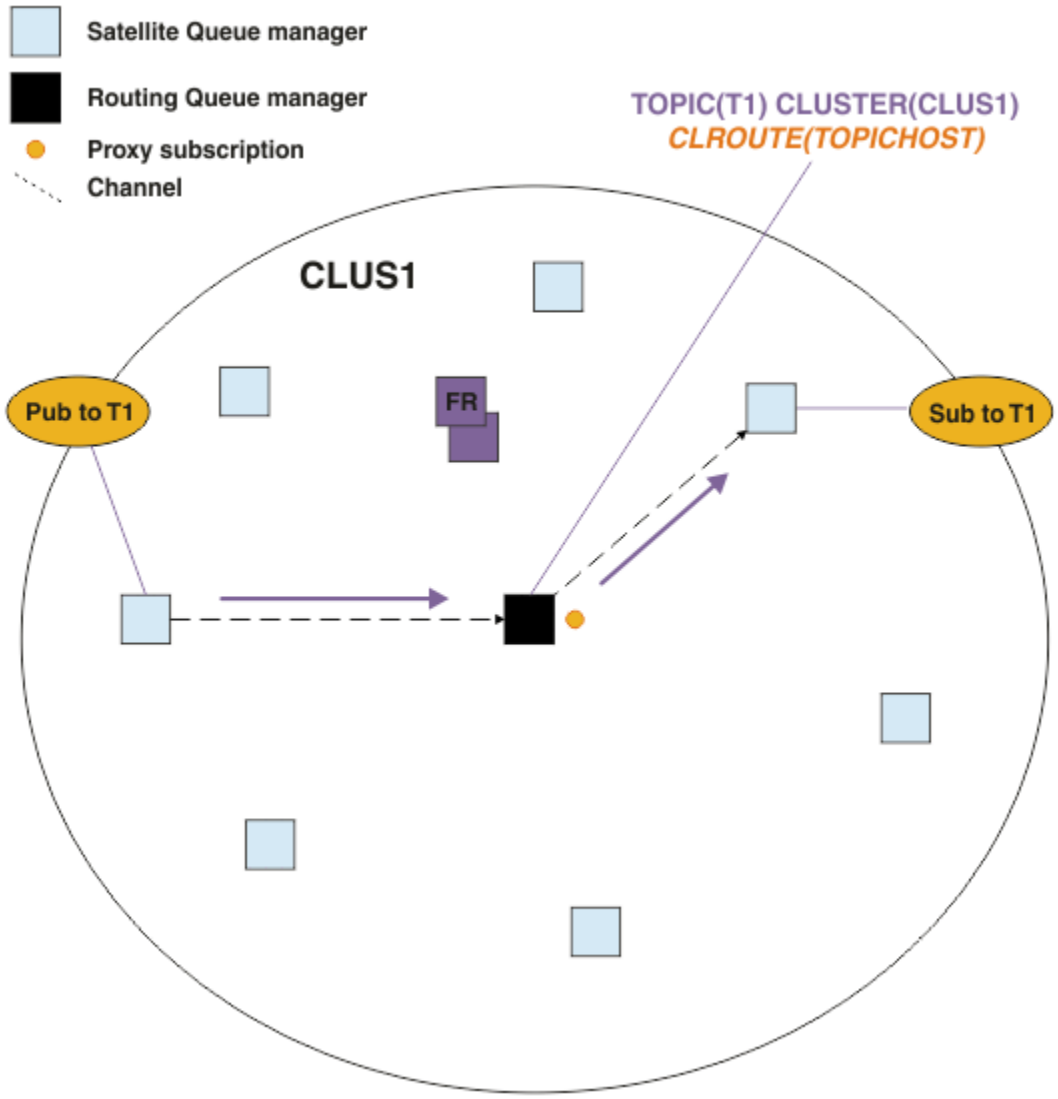


Obrázek 22. Klastr publikování/odběru směrovaný hostitelem tématu s jedním tématem definovaným na jednom hostiteli tématu a jedním odběratelem.

Když se aplikace publikování připojí k jinému správci front a je publikována zpráva, vytvoří se kanál mezi správcem front publikování a správcem front hostitele tématu a zpráva se předá tomuto správci front. Správce front publikování nemá žádné informace o odběrech jiných správců front v klastru, takže zpráva je předána správci front hostitele tématu i v případě, že pro dané téma v klastru nejsou žádní odběratelé. Správce front publikování se připojuje pouze ke správci front hostitele tématu. Publikování jsou směrována prostřednictvím hostitele tématu do správců front odběru, pokud existují.

Odběry ve stejném správci front jako vydavatel jsou uspokojeny přímo, aniž by byly nejprve odesílány zprávy správci front hostitele tématu.

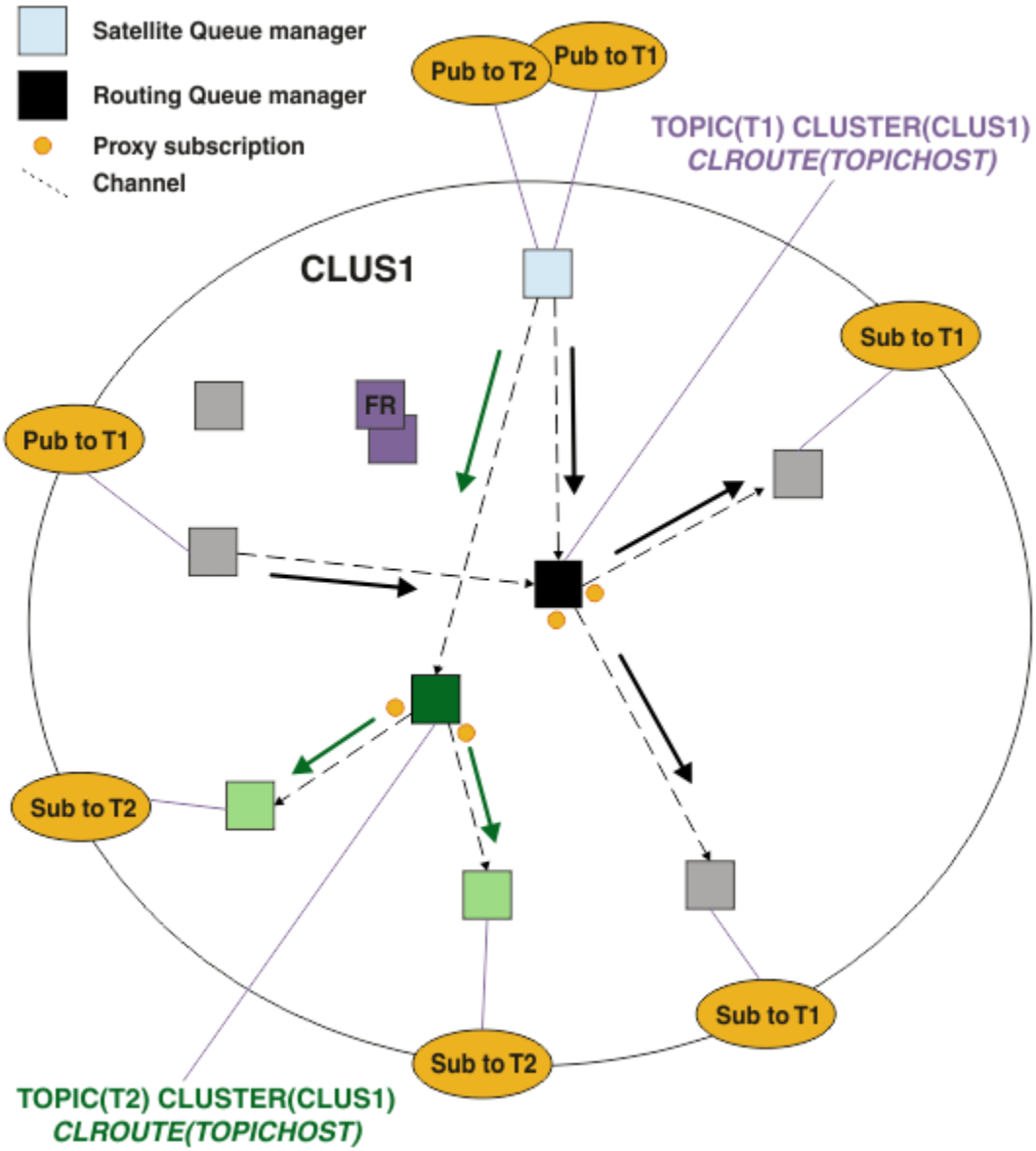
Mějte na paměti, že vzhledem ke kritické roli, kterou hraje každý správce front hostitele tématu, musíte zvolit správce front, kteří budou schopni zpracovat požadavky na zátěž, dostupnost a konektivitu pro hostování témat.



Obrázek 23. Klastr publikování/odběru směrovaný hostitelem tématu s jedním tématem, jedním odběratelem a jedním vydavatelem.

Rozdělení stromu témat mezi více správců front

Směrované téma, které je hostitelem správce front, odpovídá pouze za znalosti odběru a zprávy publikování týkající se větve stromu témat, pro kterou je konfigurován příslušný spravovaný objekt tématu. Pokud různé aplikace publikování/odběru v klastru používají různá témata, můžete nakonfigurovat různé správce front tak, aby hostili různé klastrované větve stromu témat. To umožňuje škálování tím, že se sníží provoz publikování, znalosti odběru a kanály pro každého správce front hostitele tématu v klastru. Tuto metodu byste měli použít pro různé větve velkých objemů stromu témat:



Obrázek 24. Klastr publikování/odběru směrovaný hostitelem tématu se dvěma tématy, z nichž každé je definováno na jednom hostiteli tématu.

Pokud například pomocí témat popsaných v tématu Stromy tématbylo téma T1 nakonfigurováno s řetězcem tématu `/USA/Alabamaa` téma T2 bylo nakonfigurováno s řetězcem tématu `/USA/Alaska`, pak by zpráva publikovaná do adresáře `/USA/Alabama/Mobile` byla směrována prostřednictvím správce front, který je hostitelem T1, a zpráva publikovaná do adresáře `/USA/Alaska/Juneau` bude směrována prostřednictvím správce front, který je hostitelem T2.

Poznámka: Jeden odběr nelze převést na více klastrovaných větví stromu témat pomocí zástupného znaku výše ve stromu témat, než jsou klastrované body. Viz Odběry zástupného znaku.

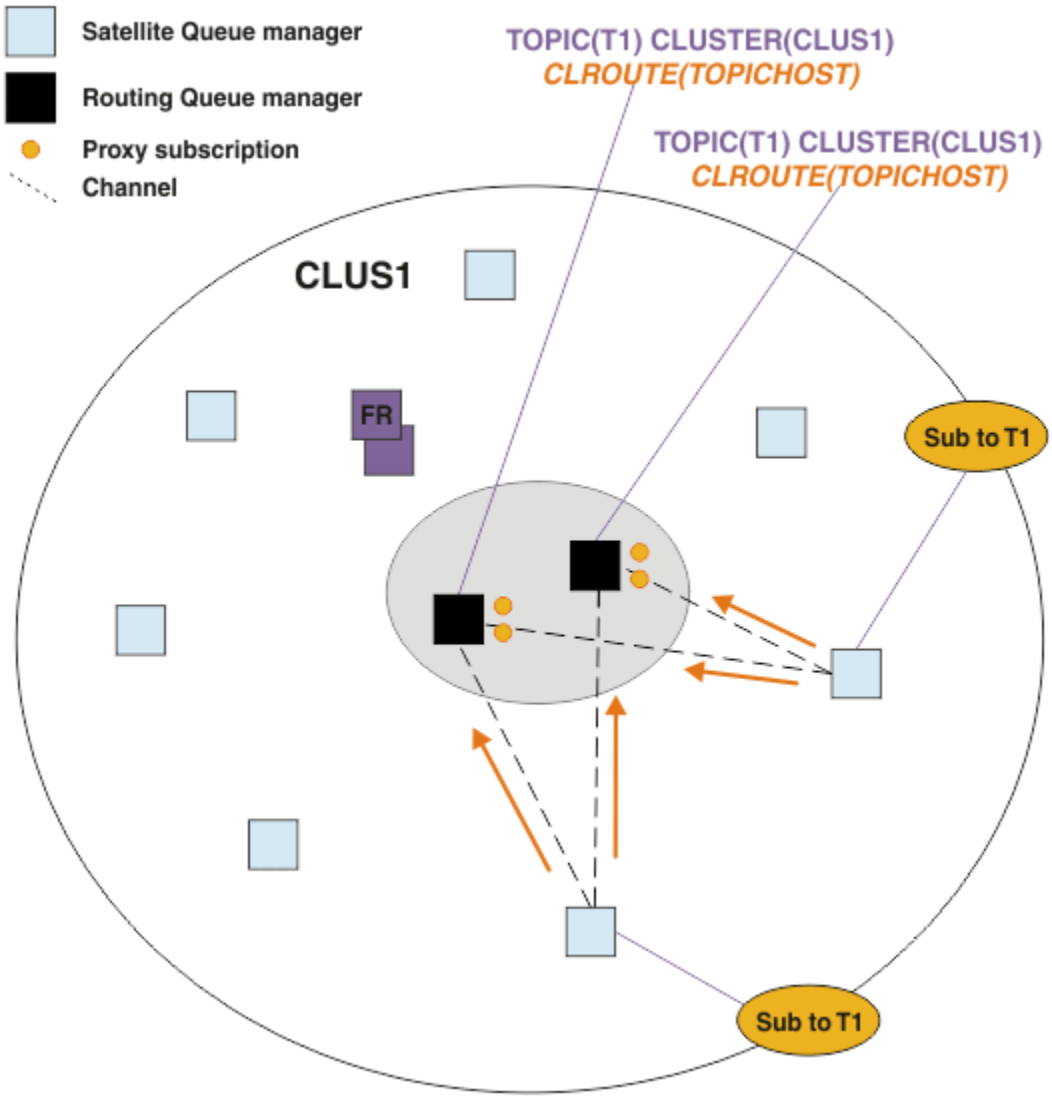
Směrování hostitelů témat pomocí více hostitelů témat pro jedno téma

Pokud jeden správce front odpovídá za směrování tématu a tento správce front nebude k dispozici nebo nebude schopen zpracovat pracovní zátěž, nebudou publikování okamžitě přesměrovávat na odběry.

Potřebujete-li větší odolnost, rozšiřitelnost a vyrovnávání pracovní zátěže, než jaké jste získali při definování tématu pouze v jednom správci front, můžete definovat téma ve více než jednom správci front. Každá jednotlivá publikovaná zpráva je směrována prostřednictvím jednoho hostitele tématu. Pokud existuje více odpovídajících definic hostitele tématu, je vybrán jeden z hostitelů tématu. Volba

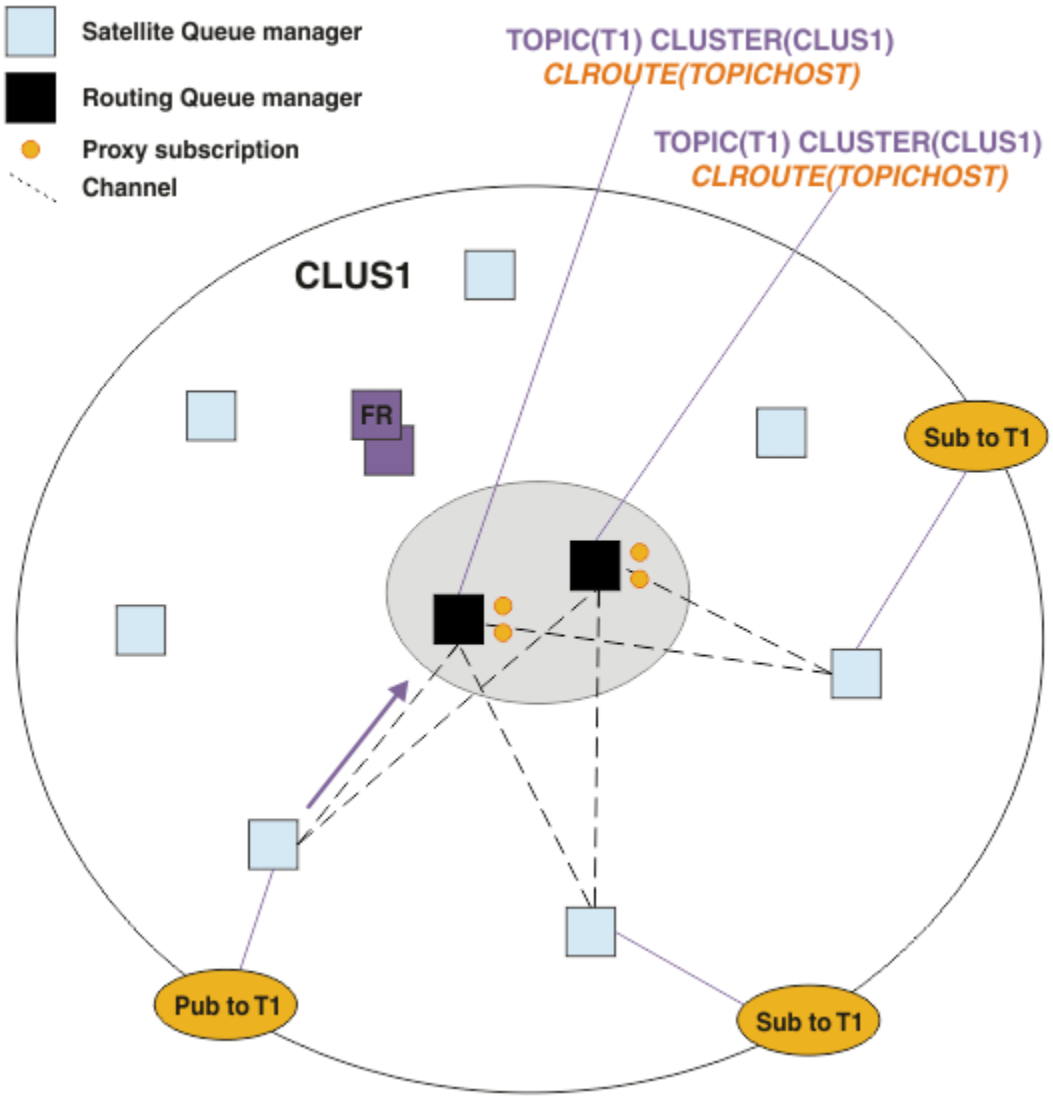
je provedena stejným způsobem jako pro klastrované fronty. To umožňuje směrování zpráv na dostupné hostitele témat, čímž se vyhnete nedostupným zprávám, a umožňuje vyrovnávání zátěže zpráv v rámci více správců front a kanálů hostitele témat. Řazení mezi více zprávami však není udržováno, pokud pro stejné téma v klastru používáte více hostitelů témat.

V následujícím diagramu je zobrazen klastr se směrovaným hostitelem tématu, v němž bylo stejné téma definováno ve dvou správcích front. V tomto příkladu odebírající správci front odesílají informace o odebíraném tématu oběma správcům front hostitele tématu ve formě proxy odběru:



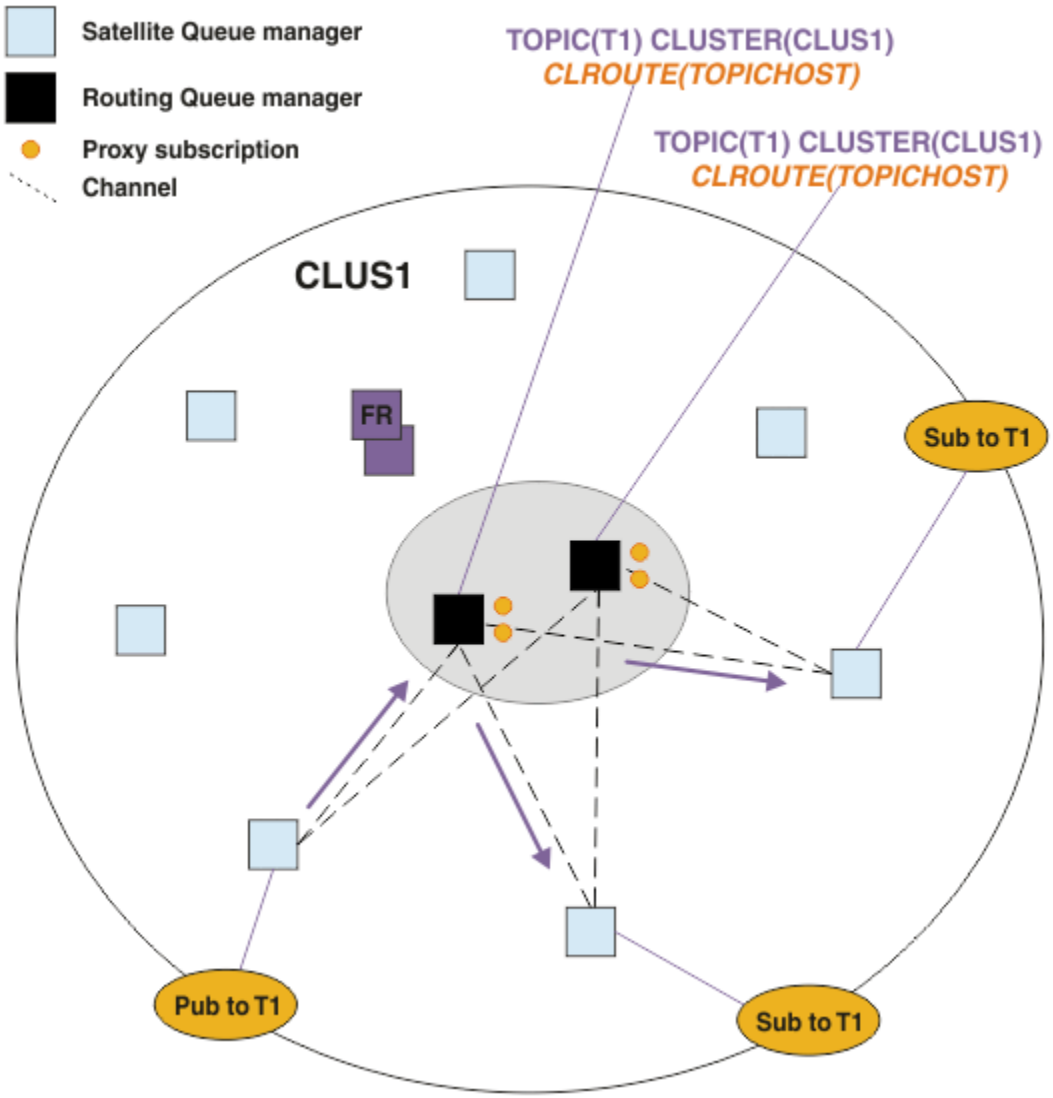
Obrázek 25. Vytvoření proxy odběrů v klastru pro publikování/odběr více hostitelů témat

Když je publikace vytvořena z nehostitelského správce front, odešle správce front kopii publikace *jednomu* ze správců front hostitele tématu pro dané téma. Systém zvolí hostitele na základě výchozího chování algoritmu správy pracovní zátěže klastru. V typickém systému se jedná o přibližnou distribuci typu round-robin v rámci každého správce front hostitele tématu. Mezi zprávami ze stejné publikační aplikace neexistuje žádná afinita. To se rovná použití typu vazby klastru `NOTFIXED`.



Obrázek 26. Příjem publikování ve více klastrech publikování/odběru hostitele tématu

Příchozí publikování pro vybraného správce front hostitele tématu jsou poté předána všem správcům front, kteří zaregistrovali odpovídající proxy odběr:



Obrázek 27. Směrování publikování odběratelům v klastru pro publikování/odběr s více hostiteli tématu

Vytváření odběrů a vydavatelů lokálních pro správce front hostitele tématu

Výše uvedené příklady ukazují směrování mezi vydavateli a odběrateli ve správcích front, kteří nehostují spravované objekty tématu se směrováním. V těchto topologiích zprávy vyžadují k dosažení odběrů více *přechodů* .

V případě, že další přechod není žádoucí, může být vhodné připojit vydavatele klíčů k tématům hostujícím správce front. Pokud však existuje více hostitelů témat pro téma a pouze jeden vydavatel, bude veškerý provoz publikování směrován prostřednictvím správce front hostitele témat, ke kterému je vydavatel připojen.

Podobně, pokud existují odběry klíčů, mohou být umístěny ve správci front hostitele tématu. Pokud však existuje více hostitelů směrovaných témat, pouze část publikací se vyvaruje dalšího přechodu, přičemž zbytek je nejprve směrován prostřednictvím jiných správců front hostitele tématu.

Níže jsou popsány topologie, jako jsou tyto: Směrování hostitelů témat pomocí centralizovaných vydavatelů nebo odběratelů.

Poznámka: Při změně konfigurace směrovaných témat při společné lokalizaci vydavatelů nebo odběrů s hostiteli směrovaných témat je zapotřebí speciální plánování. Viz například téma Přidání dalších hostitelů témat do klastru se směrovaným hostitelem tématu.

Souhrn a další aspekty

Klastr publikování/odběru se směrovaným hostitelem tématu poskytuje přesnou kontrolu nad tím, kteří správci front jsou hostiteli jednotlivých témat, a tito správci front se stávají *směrovacími* správci front pro danou větev stromu témat. Správci front bez odběrů nebo vydavatelů se navíc nemusí připojovat ke správcům front hostitele tématu a správci front s odběry se nemusí připojovat ke správcům front, kteří nejsou hostiteli tématu. Tato konfigurace může výrazně snížit počet připojení mezi správci front v klastru a množství informací předávaných mezi správci front. To platí zejména pro velké klastry, kde pouze podmnožina správců front provádí práci publikování/odběru. Tato konfigurace vám také poskytuje určitou kontrolu nad zátěží jednotlivých správců front v klastru, takže (například) se můžete rozhodnout hostovat vysoce aktivní témata na výkonnějších a odolnějších systémech. Pro určité konfigurace-zejména pro větší klastry-se obvykle jedná o vhodnější topologii než *přímé směrování*.

Avšak směrování hostitelů témat přináší do vašeho systému také určitá omezení:

- Konfigurace systému a jeho údržba vyžadují více plánování, než je tomu u přímého směrování. Musíte rozhodnout, co ukazuje ve stromu témat na klastr i o umístění definic témat v klastru.
- Stejně jako v případě přímého směrování témat se v okamžiku, kdy je nadefinováno nové téma se směrovaným hostitelem tématu, přenesou informace do správců front úplného úložiště a odtud přímo na všechny členy klastru. Tato událost způsobí spuštění kanálu pro každého člena klastru z úplných úložišť, pokud ještě nejsou spuštěny.
- Publikace se vždy posílají na správce front hostitele ze správce front mimo hostitele, a to i v případě, že v klastru neexistují žádné odběry. Proto byste měli v případech, kdy se očekává pravděpodobná existence odběrů, nebo v případech, kdy je zatížení globální konektivitou a informacemi větší než riziko nadbytečného zatížení publikacemi, používat směrovaná témata.

  Poznámka: Jak již bylo popsáno, učinit vydavatele lokálními pro hostitele tématu může toto riziko zmírnit.
- Zprávy publikované na správcích front mimo hostitele nejdou přímo na správce front, který je hostitelem odběru, ale jsou vždy směrovány skrze správce front hostitele. Tímto způsobem lze snížit celkovou režii klastru, zvýšit latenci zpráv a snížit výkon.

  Poznámka: Jak bylo popsáno dříve, vytvoření odběrů nebo vydavatelů lokálních pro hostitele tématu může toto riziko zmírnit.
- Použití jediného správce front hostitele představuje slabé místo pro všechny zprávy publikované v rámci tématu. Toto slabé místo můžete posílit definováním více hostitelů témat. Avšak použití více hostitelů ovlivňuje pořadí publikovaných zpráv přijatých podle odběrů.
- Správci front hostitelů tématu zaznamenali dodatečné zatížení zprávami, protože tito správci front museli zpracovat publikace z více správců front. Toto zatížení lze snížit - ať už použitím více hostitelů témat pro jedno téma (v takovém případě není pořadí zpráv zachováno), nebo použitím různých správců front, kteří budou hostiteli směrovaných témat pro různé větve stromu témat.

Před použitím směrování hostitelů témat prozkoumejte alternativní přístupy, které jsou podrobně popsány v části “Přímé směrování v klastrech publikování/odběru” na stránce 74a “Směrování v hierarchiích publikování/odběru” na stránce 102.

Klastrování publikování/odběru: Doporučené postupy

Použití klastrovaných témat usnadňuje rozšíření domény publikování/odběru mezi správci front, ale může vést k problémům, pokud mechanici a důsledky nejsou plně pochopeny. Existují dva modely sdílení informací a směrování publikování. Implementujte model, který nejlépe vyhovuje vašim individuálním obchodním potřebám a nejlépe funguje na vybraném klastru.

Informace o nejlepších postupech v následujících oddílech neposkytují jednu velikost pro všechna řešení, ale spíše sdílí společné přístupy k řešení společných problémů. Předpokládá, že máte základní znalost klastrů IBM MQ a systému zpráv publikování/odběru a že jste obeznámeni s informacemi v distribuovaných sítích publikování/odběru a “Návrh klastrů publikování/odběru” na stránce 72.

Používáte-li klastr pro systém zpráv typu point-to-point, pracuje každý správce front v klastru podle potřeby. To znamená, že se dozví pouze o jiných prostředcích klastru, například o jiných správcích front v klastru a klastrovaných frontách, když aplikace, které se k nim připojují, požádají o jejich použití. Při

přidávání systému zpráv publikování/odběru do klastru je zavedena zvýšená úroveň sdílení informací a konektivity mezi správci front klastru. Chcete-li se řídit doporučenými postupy pro klastry publikování/odběru, musíte plně porozumět důsledkům této změny v chování.

Chcete-li na základě přesných potřeb sestavit nejlepší architekturu, existují dva modely pro sdílení informací a směrování publikování v klastrech publikování/odběru: *přímé směrování* a *směrování hostitele tématu*. Chcete-li provést správnou volbu, musíte porozumět oběma modelům a různým požadavkům, které každý model splňuje. Tyto požadavky jsou popsány v následujících oddílech ve spojení s "Plánování distribuované sítě publikování/odběru" na stránce 69:

- "Důvody pro omezení počtu správců front klastru zapojených do aktivity publikování/odběru" na stránce 89
- "Jak se rozhodnout, která témata se mají klastrovat" na stránce 89
- "Jak zvětšit velikost systému" na stránce 90
- "Umístění vydavatele a odběru" na stránce 91
- "Provoz publikování" na stránce 91
- "Změna odběru a dynamické řetězce témat" na stránce 92

Důvody pro omezení počtu správců front klastru zapojených do aktivity publikování/odběru

Při použití systému zpráv publikování/odběru v klastru existují aspekty týkající se kapacity a výkonu. Proto je vhodné pečlivě zvážit potřebu aktivity publikování/odběru pro všechny správce front a omezit ji pouze na počet správců front, kteří ji vyžadují. Po identifikaci minimální sady správců front, kteří potřebují publikovat témata a přihlásit se k odběru témat, je možné je nastavit jako členy klastru, který obsahuje pouze tato témata, a nikoli jiné správce front.

Tento přístup je zvláště užitečný, pokud máte zavedený klastr, který již dobře funguje pro systém zpráv typu point-to-point. Když přeměňujete existující velký klastr na klastr publikování/odběru, je lepší nejprve vytvořit samostatný klastr pro práci publikování/odběru, kde lze zkoušet aplikace, spíše než použít aktuální klastr. Můžete použít podmnožinu existujících správců front, kteří jsou již v jednom či více klastrech typu point-to-point, a učinit z této podmnožiny členy nového klastru publikování/odběru. Správci front úplného úložiště pro nový klastr však nesmí být členy žádného jiného klastru; tím se izoluje další zátěž od existujících úplných úložišť klastru.

Pokud nemůžete vytvořit nový klastr a musíte změnit existující velký klastr na klastr publikování/odběru, nepoužívejte přímo směrovaný model. Model směrování hostitele tématu obvykle funguje lépe ve větších klastrech, protože obecně omezuje sdílení informací publikování/odběru a konektivitu na sadu správců front, kteří aktivně provádějí práci publikování/odběr, a soustředí se na správce front, kteří jsou hostiteli témat. Výjimkou je případ, kdy je ve správci front, který je hostitelem definice tématu, vyvolána ruční aktualizace informací o odběru. V tomto okamžiku se správce front hostitele tématu připojí ke všem správcům front v klastru. Viz Resynchronizace proxy odběrů.

Pokud zjistíte, že klastr nelze použít pro publikování/odběr kvůli jeho velikosti nebo aktuální zátěži, je vhodné zabránit neočekávanému vytvoření tohoto klastru do klastru publikování/odběru. Pomocí vlastnosti správce front **PSCLUS** zastavte všechny osoby, které přidávají klastrované téma k libovolnému správci front v klastru. Viz "Blokování klastrovaného publikování/odběru" na stránce 98.

Jak se rozhodnout, která témata se mají klastrovat

Je důležité pečlivě vybrat, která témata se přidají do klastru: Čím vyšší je strom témat, tím rozšířenější je jejich použití. To může vést k šíření více informací o odběru a publikování, než je nutné. Existuje-li více různých větví stromu témat, kde některé potřebují být klastrovány a jiné ne, vytvořte spravované objekty tématu v kořenovém adresáři každé větve, která potřebuje klastrování, a přidejte je do klastru. Pokud například větve `/A`, `/B` a `/C` potřebují klastrování, definujte pro každou větev samostatné objekty klastrovaného tématu.

Poznámka: Systém vám zabrání v vnoření definic klastrovaných témat do stromu témat. Témata můžete klastrovat pouze v jednom bodě stromu témat pro každou dílčí větev. Nemůžete například definovat

klastrované objekty témat pro /A a pro /A/B. Vnoření klastrovaných témat může vést k nejasnostem ohledně toho, který klastrovaný objekt se týká kterého odběru, zejména pokud odběry používají zástupné znaky. To je ještě důležitější při použití směrování hostitelů témat, kde jsou rozhodnutí o směrování přesně definována přidělením hostitelů témat.

Pokud musí být klastrovaná témata přidána ve stromu témat výše, ale některé větve stromu pod klastrovaným bodem nevyžadují klastrované chování, můžete použít atributy rozsahu odběru a publikování ke snížení úrovně odběru a sdílení publikování pro další témata.

Kořenový uzel tématu byste neměli vkládat do klastru, aniž byste zohledňovali chování, které vidíte. Globální témata jsou zřejmá všude, kde je to možné, například pomocí kvalifikátoru vyšší úrovně v řetězci tématu: `/global` nebo `/cluster`.

Existuje další důvod, proč se nechce nastavit uzel kořenového tématu jako klastrovaný. Důvodem je, že každý správce front má lokální definici pro kořenový uzel, objekt tématu `SYSTEM.BASE.TOPIC`. Je-li tento objekt klastrován v jednom správci front v klastru, budou o něm informováni všichni ostatní správci front. Pokud však existuje lokální definice stejného objektu, jeho vlastnosti přepíší objekt klastru. Výsledkem jsou správci front, kteří se chovají, jako by téma nebylo klastrováno. Chcete-li to vyřešit, musíte klastrovat každou definici `SYSTEM.BASE.TOPIC`. To lze provést pro definice s přímým směrovaným pořadem, ale nikoli pro definice hostitele tématu s směrovaným pořadem, protože to způsobí, že se každý správce front stane hostitelem tématu.

Jak zvětšit velikost systému

Klastry publikování/odběru obvykle vedou k odlišnému vzoru kanálů klastru pro systém zpráv typu point-to-point v klastru. Dvoubodový model je "opt in", ale klastry publikování/odběru mají nerozlišitelnější charakter s rozložením odběrů, zejména při použití přímo směrovaných témat. Proto je důležité identifikovat, kteří správci front v klastru publikování/odběru budou používat kanály klastru pro připojení k jiným správcům front a za jakých okolností.

V následující tabulce je uvedena typická sada odesílacích a přijímacích kanálů klastru očekávaná pro každého správce front v klastru publikování/odběru za normálního spuštění v závislosti na roli správce front v klastru publikování/odběru.

Tabulka 5. Odesílací a přijímací kanály klastru pro každou metodu směrování.

Role správce front	Přímí příjemci klastru	Přímí odesilatelé klastrů	Příjemci klastru témat	Odesilatelé klastrů témat
Úložiště souborů	AllQmgrs	AllQmgrs	AllQmgrs	AllQMgrs
Hostitel definice tématu	Není k dispozici.	Není k dispozici.	AllSubs+AllPubs (1)	AllSubs (1)
Vytvořené odběry	AllPubs (1)	AllQMgrs	AllHosts	AllHosts
Připojení vydavatelé	AllSubs (1)	AllSubs (1)	AllHosts	AllHosts
Žádní vydavatelé nebo odběratelé	AllSubs (1)	Žádné (1)	Žádné (2)	Žádné (2)

Klíč:

AllQmgrs
Kanál do a z každého správce front v klastru.

AllSubs
Kanál do a ze všech správců front, kde byl vytvořen odběr.

AllPubs
Kanál do a z každého správce front, ke kterému byla připojena publikační aplikace.

AllHosts
Kanál do a z každého správce front, kde byla konfigurována definice klastrovaného objektu tématu.

Není
Pro výhradní účely systému zpráv publikování/odběru nejsou k dispozici žádné kanály pro jiné správce front v klastru ani z nich.

Notes:

1. Pokud je provedena aktualizace správce front proxy odběrů z tohoto správce front, může být automaticky vytvořen kanál do všech ostatních správců front v klastru a ze všech ostatních správců front v klastru.
2. Pokud je z tohoto správce front vytvořena aktualizace správce front proxy odběrů, může být automaticky vytvořen kanál pro všechny další správce front v klastru, který je hostitelem definice klastrovaného tématu.

Předchozí tabulka ukazuje, že směrování hostitelů témat obvykle používá výrazně méně odesílacích a přijímacích kanálů klastru než přímé směrování. Pokud je konektivita kanálu pro určité správce front v klastru znepokojivá, z důvodů kapacity nebo schopnosti vytvořit určité kanály (například prostřednictvím bran firewall), je směrování hostitele tématu preferovaným řešením.

Umístění vydavatele a odběru

Klastrované publikování/odběr umožňuje, aby zprávy publikované v jednom správci front byly doručeny k odběrům v libovolném jiném správci front v klastru. Pokud jde o dvoubodový systém zpráv, náklady na přenos zpráv mezi správci front mohou mít nepříznivý dopad na výkon. Proto byste měli zvážit vytvoření odběrů témat ve stejných správcích front, v nichž jsou zprávy publikovány.

Při použití směrování hostitelů témat v rámci klastru je důležité zvážit také umístění odběrů a vydavatelů s ohledem na téma hostující správce front. Není-li vydavatel připojen ke správci front, který je hostitelem klastrovaného tématu, budou publikované zprávy vždy odesílány do tématu, které je hostitelem správce front. Podobně při vytvoření odběru ve správci front, který není hostitelem tématu pro klastrované téma, jsou zprávy publikované z jiných správců front v klastru vždy nejprve odesílány do tématu, které je hostitelem správce front. Přesněji řečeno, pokud je odběr umístěn ve správci front, který je hostitelem tématu, ale existuje jeden nebo více správců front, kteří jsou hostiteli téhož tématu, bude část publikování z jiných správců front směrována prostřednictvím těchto jiných správců front, kteří jsou hostiteli témat. Další informace o návrhu klastru publikování/odběru se směrováním hostitele tématu s cílem minimalizovat vzdálenost mezi vydavateli a odběry naleznete v tématu Směrování hostitelů témat pomocí centralizovaných vydavatelů nebo odběratelů .

Provoz publikování

Zprávy publikované aplikací připojenou k jednomu správci front v klastru jsou přenášeny k odběrům v jiných správcích front pomocí odesílacích kanálů klastru.

Používáte-li přímé směrování, budou publikované zprávy používat nejkratší cestu mezi správci front. To znamená, že jdou přímo ze správce front publikování do všech správců front s odběry. Zprávy nejsou přenášeny do správců front, kteří nemají odběry pro dané téma. Viz Odběry proxy v síti publikování/odběru.

Pokud je rychlost publikování zpráv mezi kterýmikoli správcem front a jiným správcem front v klastru vysoká, infrastruktura kanálu klastru mezi těmito dvěma body musí být schopna tuto rychlost zachovat. To může zahrnovat vyladění používaných kanálů a přenosové fronty.

Při použití směrování hostitele tématu je každá zpráva publikovaná ve správci front, který není hostitelem tématu, přenesena do správce front hostitele tématu. Tato volba je nezávislá na tom, zda jeden nebo více odběrů existuje kdekoli jinde v klastru. To zavádí další faktory, které je třeba zvážit při plánování:

- Je další latence prvního odeslání jednotlivých publikací správci front hostitele tématu přijatelná?
- Může každý správce front hostitele tématu udržovat četnost příchozích a odchozích publikování? Zvažte systém s vydavateli v mnoha různých správcích front. Pokud všechny odesílají své zprávy do velmi malé sady správců front hostujících témata, mohou se tito hostitelé témat stát kritickým místem při zpracování těchto zpráv a jejich směrování na odebírající správce front.

- Očekává se, že významná část publikovaných zpráv nebude mít odpovídajícího odběratele? Je-li tomu tak a rychlost publikování takových zpráv je vysoká, může být nejlepší nastavit správce front vydavatele jako hostitele tématu. V této situaci nebudou žádné publikované zprávy, ve kterých v klastru neexistují žádné odběry, přeneseny na žádné jiné správce front.

Tyto problémy mohou být také zmírněny zavedením více hostitelů témat, aby se zátěž publikování rozložila mezi ně:

- Pokud existuje více různých témat, z nichž každé má určitou část publikačního provozu, zvažte jejich hostování v různých správcích front.
- Pokud témata nelze oddělit od různých hostitelů témat, zvažte definování stejného objektu tématu ve více správcích front. To vede k tomu, že publikování jsou v rámci každého z nich vyvážena pracovní zátěží pro směrování. Toto je však vhodné pouze v případě, že není vyžadováno řazení zpráv publikování.

Změna odběru a dynamické řetězce témat

Dalším aspektem je vliv na výkon systému při šíření proxy odběrů. Správce front obvykle odesílá zprávu proxy odběru určitým jiným správcům front v klastru, když je v tomto správci front vytvořen první odběr pro specifický řetězec klastrovaného tématu (nikoli pouze konfigurovaný objekt tématu). Podobně je zpráva o odstranění proxy odběru odeslána při odstranění posledního odběru pro specifický řetězec klastrovaného tématu.

V případě přímého směrování odesílá každý správce front s odběry tyto proxy odběry všem ostatním správcům front v klastru. V případě směrování hostitelů témat odesílá každý správce front s odběry pouze proxy odběry jednotlivým správcům front, kteří jsou hostiteli definice pro dané klastrované téma. Proto při přímém směrování platí, že čím více správců front je v klastru, tím vyšší je režie při údržbě proxy odběrů v rámci klastru. Vzhledem k tomu, že při směrování hostitelů témat není počet správců front v klastru faktorem.

V obou modelech směrování platí, že pokud se řešení publikování/odběru skládá z mnoha jedinečných řetězců témat, k jejichž odběru je přihlášeno, nebo pokud jsou témata ve správci front v klastru často odebíraná a odebíraná, bude na tomto správci front patrná značná režie, která je způsobena neustálým generováním zpráv distribuujících a odstraňujících proxy odběry. Při přímém směrování je to komplikovaných potřebou odeslat tyto zprávy všem správcům front v klastru.

Je-li četnost změn odběrů příliš vysoká na to, aby ji bylo možné přizpůsobit, a to i v rámci systému se směrovaným hostitelem tématu, informace o způsobech snížení režie proxy odběrů naleznete v tématu Výkon odběru v sítích publikování/odběru .

Definování témat klastru

Témata klastru jsou administrativní témata s definovaným atributem **`cluster`** . Informace o tématech klastru se publikují na všechny členy klastru a v kombinaci s lokálními tématy vytváří části prostoru témat, které pokrývají více správců front. Tato konfigurace umožňuje publikovat zprávy k tématu na jednom správci front, a doručení těchto zpráv do odběrů na ostatních správcích front v klastru.

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 následně použít libovolný správce front v klastru, ale veškeré změny v tomto tématu klastru se musí provádět na tom správci front, na kterém bylo toto téma nadefinováno (na hostiteli), načež se tyto změny rozšíří na všechny členy klastru prostřednictvím úplných úložišť.

Při použití přímého směrování nemá umístění definice klastrovaného tématu přímý vliv na chování systému, protože všichni správci front v klastru používají definici tématu stejným způsobem. Proto byste měli definovat téma pro každého správce front, který bude členem klastru tak dlouho, dokud bude téma potřeba, a to v systému, který je dostatečně spolehlivý, aby mohl být pravidelně v kontaktu se správci front úplného úložiště.

Při použití směrování hostitelů témat je velmi důležité umístění definice klastrovaného tématu, protože ostatní správci front v klastru vytvářejí kanály pro tohoto správce front a odesílají do něj informace

o odběru a publikování. Chcete-li vybrat nejlepšího správce front, který bude hostitelem definice tématu, musíte porozumět směrování hostitele tématu. Viz “Směrování hostitelů témat v klastrech publikování/odběru” na stránce 79.

Máte-li klastrované téma a lokální objekt tématu, má přednost lokální téma. Viz “Více definic témat klastru se stejným názvem” na stránce 95.

Informace o příkazech používaných k zobrazení témat klastru viz související informace.

Dědičnost klastrovaných témat

Publikování a odběr aplikací v klastrované topologii publikování/odběru obvykle očekávají, že budou pracovat stejně, bez ohledu na to, ke kterému správci front v klastru jsou připojeni. Proto jsou objekty klastrovaných spravovaných témat šířeny do všech správců front v klastru.

Spravovaný objekt tématu dědí své chování od ostatních spravovaných objektů tématu ve stromu témat. K této dědičnosti dochází v případě, že pro parametr tématu nebyla nastavena explicitní hodnota.

V případě klastrovaného publikování/odběru je důležité zvážit tuto dědičnost, protože zavádí možnost, že se vydavatelé a odběratelé budou chovat odlišně v závislosti na tom, ke kterému správci front se připojují. Pokud objekt klastrovaného tématu ponechá všechny parametry, které mají dědit z vyšších objektů tématu, může se téma v různých správcích front v klastru chovat odlišně. Podobně lokálně definované objekty tématu definované pod klastrovaným objektem tématu ve stromu témat budou znamenat, že tato nižší témata budou stále klastrována, ale lokální objekt může změnit své chování způsobem, který se liší od ostatních správců front v klastru.

Zástupné odběry

Proxy odběry jsou vytvořeny, když jsou lokální odběry vytvořeny pro řetězec tématu, který se interpretuje v klastrovaném objektu tématu nebo pod ním. Pokud je odběr se zástupnými znaky v hierarchii témat vyšší než jakékoli téma klastru, nemá proxy odběry odesílané kolem klastru pro odpovídající téma klastru, a proto nepřijímá žádná publikování od ostatních členů klastru. Přijímá však publikování od lokálního správce front.

Pokud se však jiná aplikace přihlásí k odběru řetězce tématu, který je přeložen do tématu klastru nebo pod ním, jsou generovány proxy odběry a publikování jsou šířena do tohoto správce front. Po příchodu originálu je vyšší předplatné se zástupnými znaky považováno za oprávněného příjemce těchto publikací a obdrží kopii. Pokud toto chování není vyžadováno, nastavte v klastrovaném tématu hodnotu **`WILDCARD(BLOCK)`** . To způsobí, že původní zástupný znak nebude považován za legitimní odběr, a zastaví příjem všech publikací (lokálních nebo odjinud v klastru) na téma klastru nebo jeho dílčí témata.

Související pojmy

Práce s administrativními tématy

Práce s odběry

Související odkazy

DISPLAYTOPIC-zobrazení

DISPLAYTPSTATUS

DISPLAYSUB-zobrazení

Atributy tématu klastru

Má-li objekt tématu nastaven atribut názvu klastru, bude definice tématu šířena mezi všemi správci front v klastru. Každý správce front používá atributy šířeného tématu k řízení chování aplikací publikování/odběru.

Objekt tématu má řadu atributů, které platí pro klastry publikování/odběru. Některé řídí obecné chování publikačních a odebírajících aplikací a některé řídí způsob použití tématu v rámci klastru.

Definice klastrovaného objektu tématu musí být nakonfigurována tak, aby ji všichni správci front v klastru mohli správně používat.

Například v případě modelových front, které mají být použity pro spravované odběry (MDURMDL a MNDURMDL). jsou nastaveny na jiný než výchozí název fronty, který musí být definován ve všech správcích front, kde budou vytvořeny spravované odběry.

Podobně, je-li některý atribut nastaven na hodnotu ASPARENT, bude chování tématu záviset na vyšších uzlech ve stromu témat (viz Objekty administrativních témat). na každém jednotlivém správci front v klastru. To může vést k odlišnému chování při publikování nebo přihlášení k odběru z různých správců front.

Hlavní atributy, které přímo souvisí s chováním publikování/odběru v rámci klastru, jsou následující:

CLROUTE
Tento parametr řídí směrování zpráv mezi správci front, v nichž jsou připojeni vydavatelé, a správci front, v nichž existují odpovídající odběry.

- Trasu nakonfigurujete tak, aby byla buď přímá mezi těmito správci front, nebo prostřednictvím správce front, který je hostitelem definice klastrovaného tématu. Další podrobnosti viz Klastry publikování/odběru .
- Parametr **CLROUTE** nelze změnit, je-li nastaven parametr **CLUSTER** . Chcete-li změnit **CLROUTE**, nejprve nastavte vlastnost **CLUSTER** na prázdnou hodnotu. To zastaví aplikace, které používají toto téma, aby se chovaly klastrovaným způsobem. To zase vede k přerušení publikování doručovaných odběrům, takže byste měli při provádění změn také uvést systém zpráv publikování/odběru do klidového stavu.

PROXYSUB
Tento parametr určuje, kdy jsou prováděny proxy odběry.

- FIRSTUSE je výchozí hodnota a způsobuje, že proxy odběry jsou odesílány jako odpověď na lokální odběry ve správci front v distribuované topologii publikování/odběru a zrušeny, pokud již nejsou vyžadovány. Podrobnosti o tom, proč byste mohli chtít změnit tento atribut z výchozí hodnoty FIRSTUSE, viz Individuální předávání proxy odběrů a *publikovat všude* .
- Chcete-li povolit *publikovat všude*, nastavte parametr **PROXYSUB** na FORCE pro objekt tématu vysoké úrovně. Výsledkem je jeden proxy odběr se zástupnými znaky, který odpovídá všem tématům pod tímto objektem tématu ve stromu témat.

Poznámka: Nastavení atributu **PROXYSUB(FORCE)** ve velkém nebo zaneprázdněném klastru publikování/odběru může vést k nadměrnému zatížení systémových prostředků. Atribut **PROXYSUB(FORCE)** je rozšířen na všechny správce front, nikoli pouze na správce front, pro kterého bylo téma definováno. To způsobí, že každý správce front v klastru vytvoří proxy odběr se zástupnými znaky.

Kopie zprávy do tohoto tématu, publikovaná v libovolném správci front v klastru, je odeslána všem správcům front v klastru-buď přímo, nebo prostřednictvím správce front hostitele tématu, v závislosti na nastavení **CLROUTE** .

Při přímém směrování tématu vytvoří každý správce front odesílací kanály klastru pro každého jiného správce front. Je-li téma směrováno na hostitele tématu, vytvoří se kanály pro každého správce front hostitele tématu z každého správce front v klastru.

Další informace o parametru **PROXYSUB** při použití v klastrech naleznete v tématu Výkon přímého směrovaného publikování/odběru.

PUBSCOBE a SUBSCOPE
Tyto parametry určují, zda tento správce front rozšíří publikování do správců front v topologii (klastr či hierarchie publikování/odběru) nebo omezí rozsah pouze na svého lokálního správce front. Ekvivalentní úlohu můžete provést programově pomocí MQPMO_SCOPE_QMGR a MQSO_SCOPE_QMGR.

PUBSCOPE
Pokud je objekt tématu klastru definován s produktem **PUBSCOPE(QMGR)**, je definice sdílena s klastrem, ale rozsah publikování, která jsou založena na tomto tématu, je pouze lokální a nejsou odesílána jiným správcům front v klastru.

SUBSCOPE
Pokud je objekt tématu klastru definován s produktem **SUBSCOPE(QMGR)**, je definice sdílena s klastrem, ale rozsah odběrů založených na tomto tématu je pouze lokální, a proto nejsou žádné proxy odběry odesílány jiným správcům front v klastru.

Tyto dva atributy se běžně používají společně k izolování správce front od interakce s ostatními členy klastru v konkrétních tématech. Správce front nepublikuje ani nepřijímá publikace týkající se těchto témat od ostatních 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 nebrání ostatním správcům front v klastru v tom, aby šířili své proxy odběry do správce front, pokud používají klastrovanou verzi tématu s produktem **SUBSCOPE(ALL)**. Pokud však lokální definice také nastaví parametr **PUBSCOPE** na hodnotu QMGR , nebudou tyto proxy odběry odesílány z tohoto správce front.

Související pojmy
Obor publikování
Obor odběru

Více definic témat klastru se stejným názvem
Stejný pojmenovaný objekt tématu klastru můžete definovat ve více než jednom správci front v klastru a v určitých scénářích to umožňuje specifické chování. Pokud existuje více definic témat klastru se stejným názvem, většina vlastností by se měla shodovat. Pokud se tak nestane, jsou hlášeny chyby nebo varování v závislosti na významnosti neshody.

Obecně platí, že dojde-li k neshodě ve vlastnostech více definic témat klastru, budou vydána varování a každý správce front v klastru použije jednu z definic objektů tématu. Definice, kterou používá každý správce front, není deterministická nebo konzistentní v rámci správců front v klastru. Tyto neshody by měly být vyřešeny co nejrychleji.

Během nastavení nebo údržby klastru je někdy nutné vytvořit více definic témat klastru, které nejsou identické. To je však vždy užitečné pouze jako dočasné opatření, a proto je považováno za možný chybový stav.

Při zjištění neshod jsou do protokolu chyb jednotlivých správců front zapsány následující varovné zprávy:

- Multi V Multiplatforms, AMQ9465 a AMQ9466.
- z/OS V systémech z/OS, CSQX465I a CSQX466I.

Vybrané vlastnosti pro libovolný řetězec tématu v jednotlivých správcích front lze určit zobrazením stavu tématu namísto definic objektů tématu, například pomocí **DISPLAY TPSTATUS**.

V některých situacích je konflikt ve vlastnostech konfigurace natolik závažný, že zastavuje vytvářený objekt tématu nebo způsobuje, že neshodné objekty jsou označeny jako neplatné a nejsou šířeny napříč klastrem (viz **CLSTATE** v DISPLAY TOPIC). K těmto situacím dochází, když dojde ke konfliktu ve vlastnosti směrování klastru (**CLROUTE**). definic témat. Vzhledem k důležitosti konzistence mezi jednotlivými definicemi hostitele tématu jsou navíc další nekonzistence odmítnuty, jak je podrobně popsáno v následujících oddílech tohoto článku.

Pokud je konflikt zjištěn v době, kdy je objekt definován, je změna konfigurace odmítnuta. Pokud budou správci front úplného úložiště později detekováni, budou do protokolů chyb správců front zapsány následující varovné zprávy:

- Multi V systému Multiplatforms: AMQ9879
- z/OS V systému z/OS: CSQX879E.

Je-li v klastru definováno více definic stejného objektu tématu, má lokálně definovaná definice přednost před jakoukoli vzdáleně definovanou definicí. Pokud tedy v definicích existují rozdíly, správci front, kteří jsou hostiteli více definic, se od sebe chovají odlišně.

Efekt definování tématu mimo klastr se stejným názvem jako téma klastru z jiného správce front

Je možné definovat administrovaný objekt tématu, který není klastrován ve správci front, který je v klastru, a současně definovat stejný pojmenovaný objekt tématu jako klastrovanou definici tématu v jiném správci front. V tomto případě má lokálně definovaný objekt tématu přednost před všemi vzdálenými definicemi se stejným názvem.

To má za následek zabránění chování klastrování tématu při použití z tohoto správce front. To znamená, že odběry nemusí přijímat publikování od vzdálených vydavatelů a zprávy od vydavatelů nemusí být šířeny na vzdálené odběry v klastru.

Před konfigurací takového systému je třeba pečlivě zvážit, protože to může vést k matoucího chování.

Poznámka: Pokud musí jednotlivý správce front zabránit šíření publikování a odběrů v rámci klastru, i když bylo téma klastrováno jinde, je alternativním přístupem nastavit rozsahy publikování a odběrů pouze na lokálního správce front. Viz “Atributy tématu klastru” na stránce 93.

Více definic témat klastru v klastru s přímým směrováním

V případě přímého směrování obvykle nedefinujete stejné téma klastru ve více než jednom správci front klastru. Důvodem je skutečnost, že přímé směrování zpřístupňuje téma všem správcům front v klastru bez ohledu na to, ve kterém správci front bylo definováno. Navíc přidání více definic témat klastru významně zvyšuje aktivitu systému a administrativní složitost a se zvýšenou složitostí je větší pravděpodobnost lidské chyby:

- Každá definice má za následek odeslání dalšího objektu tématu klastru do ostatních správců front v klastru, včetně ostatních správců front hostitele tématu klastru.
- Všechny definice pro specifické téma v klastru musí být identické, jinak je obtížné zjistit, kterou definici tématu používá správce front.

Rovněž není nutné, aby jediný správce front hostitele byl neustále k dispozici pro správné fungování tématu v rámci klastru, protože definice tématu klastru je uložena do mezipaměti správci front úplného úložiště a všemi ostatními správci front v jejich dílčích úložištích klastru. Další informace naleznete v tématu Dostupnost správců front hostitele tématu, kteří používají přímé směrování.

V případě situace, kdy může být nutné dočasně definovat téma klastru ve druhém správci front, například pokud má být existující hostitel tématu odebrán z klastru, postupujte podle tématu Přesunutí definice tématu klastru do jiného správce front.

Potřebujete-li definici tématu klastru upravit, upravujte ji ve stejném správci front, v němž byla původně definována. Při pokusu o úpravu z jiného správce front může dojít k neúmyslnému vytvoření druhé definice tématu s konfliktními atributy tématu.

Více definic tématu klastru v klastru se směrováním hostitelů témat

Je-li téma klastru definováno s trasou klastru *hostitel tématu*, bude toto téma šířeno mezi všemi správci front v klastru stejně jako u *přímých* směrovaných témat. Dále je veškerý systém zpráv publikování/odběru pro dané téma směrován prostřednictvím správců front, v nichž je dané téma definováno. Proto je důležité umístění a počet definic tématu v klastru (viz “Směrování hostitelů témat v klastrech publikování/odběru” na stránce 79).

Chcete-li zajistit odpovídající dostupnost a rozšiřitelnost, je užitečné, je-li to možné, mít více definic témat. Viz Dostupnost správců front hostitele tématu, kteří používají směrování hostitele tématu.

Při přidávání nebo odebírání dalších definic *hostitele tématu* směrovaného tématu v klastru byste měli zvážit tok zpráv v době změny konfigurace. Pokud jsou zprávy publikovány v klastru do tématu v době změny, je k přidání nebo odebrání definice tématu vyžadován fázový proces. Viz Přesunutí definice tématu klastru do jiného správce front a Přidání dalších hostitelů témat do klastru se směrovaným hostitelem tématu.

Jak již bylo vysvětleno, vlastnosti více definic by se měly shodovat, s možnou výjimkou parametru **PUB** , jak je popsáno v další části. Při směrování publikování prostřednictvím správců front hostitele tématu je ještě důležitější, aby více definic bylo konzistentní. Proto je nekonzistence zjištěná v řetězci tématu nebo v názvu klastru odmítnuta, pokud byla pro směrování klastru hostitele tématu nakonfigurována jedna nebo více definic tématu.

Poznámka: Definice témat klastru jsou také odmítnuty, pokud dojde k pokusu o jejich konfiguraci nad nebo pod jiným tématem ve stromu témat, kde je existující definice klastrovaného tématu konfigurována pro směrování hostitelů témat. Tím se zabrání nejednoznačnosti ve směrování publikací s ohledem na zástupné znaky odběrů.

Speciální obsluha pro parametr PUB

Parametr **PUB** se používá k řízení, kdy mohou aplikace publikovat do tématu. V případě směrování hostitele tématu v klastru může také řídit, kteří správci front hostitele tématu se používají ke směrování publikování. Z tohoto důvodu je povoleno mít v klastru více definic stejného objektu tématu s různými nastaveními pro parametr PUB .

Pokud má více vzdálených klastrovaných definic tématu různá nastavení pro tento parametr, toto téma umožňuje, aby byla publikování odesílána a doručována odběrům, pokud jsou splněny následující podmínky:

- Ve správci front není definován odpovídající objekt tématu, ke kterému je vydavatel připojen a který je nastaven na hodnotu `PUB(DISABLED)`.
- Jedna nebo více definic témat v klastru je nastavena na hodnotu `PUB(ENABLED)` nebo jedna či více definic témat je nastavena na hodnotu `PUB(ASPARENT)` a lokální správci front, ke kterým je připojen vydavatel a definovaný odběr, jsou ve vyšším bodě stromu témat nastaveny na hodnotu `PUB(ENABLED)` .

V případě směrování hostitelů témat platí, že pokud jsou zprávy publikovány aplikacemi připojenými ke správcům front, kteří nejsou hostiteli témat, jsou zprávy směrovány pouze ke správcům front, kteří jsou hostiteli témat, kde parametr **PUB** nebyl explicitně nastaven na hodnotu `DISABLED`. Proto můžete použít nastavení `PUB(DISABLED)` k uvedení zpráv do klidového stavu prostřednictvím určitých hostitelů témat. To může být vhodné provést při přípravě na údržbu nebo odebrání správce front nebo z důvodů popsaných v tématu Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat.

Dostupnost správců front hostitele tématu klastru
Navrhněte klastr publikování/odběru tak, aby se minimalizovalo riziko, že v případě, že by se správce front hostitele tématu stal nedostupným, nebude klastr nadále schopen zpracovat provoz pro dané téma. Vliv nedostupnosti správce front hostitele tématu závisí na tom, zda klastr používá směrování hostitele tématu nebo přímé směrování.

Dostupnost správců front hostitele tématu, kteří používají přímé směrování

V případě přímého směrování obvykle nedefinujete stejné téma klastru ve více než jednom správci front klastru. Důvodem je skutečnost, že přímé směrování zpřístupňuje téma všem správcům front v klastru bez ohledu na to, ve kterém správci front bylo definováno.Viz Vícenásobné definice témat klastru v přímo směrovaném klastru.

Kdykoli v klastru přestane být hostitel klastrovaného objektu (například klastrovaná fronta nebo klastrované téma) po delší dobu k dispozici, ostatním členům klastru nakonec vyprší platnost znalostí o těchto objektech. V případě klastrovaného tématu platí, že pokud se správce front hostitele tématu klastru stane nedostupným, budou ostatní správci front nadále zpracovávat požadavky na publikování/odběr pro dané téma přímo v clusteru (tj. odesílání publikací k odběrům ve vzdálených správcích front) po dobu nejméně 60 dnů od posledního okamžiku, kdy bylo téma hostující správce front v komunikaci se správci front úplného úložiště. Pokud správce front, v němž jste definovali objekt tématu klastru, již nikdy nebude k dispozici, budou objekty tématu uložené v mezipaměti v ostatních správcích front odstraněny a téma se vrátí k lokálnímu tématu. V takovém případě nebudou odběry přijímat publikování od aplikací připojených ke vzdáleným správcům front.

Po uplynutí 60denního období pro zotavení správce front, pro kterého definujete objekt tématu klastru, není nutné provádět zvláštní opatření, která by zaručila, že hostitel tématu klastru zůstane k dispozici (mějte však na paměti, že všechny odběry definované v nedostupném hostiteli tématu klastru nejsou k dispozici). Šedesátidenní lhůta je dostatečná pro řešení technických problémů a je pravděpodobné, že bude překročena pouze kvůli administrativním chybám. Chcete-li tuto možnost zmírnit, pokud je hostitel tématu klastru nedostupný, všichni členové klastru zapisují zprávy protokolu chyb každou hodinu, přičemž uvádějí, že jejich objekt tématu klastru uložený v mezipaměti nebyl aktualizován. Na tyto zprávy reagujte tak, že se ujistíte, že je spuštěn správce front, pro kterého je definován objekt tématu klastru. Pokud není možné znovu zpřístupnit správce front hostitele tématu klastru, definujte stejnou definici klastrovaného tématu s přesně stejnými atributy v jiném správci front v klastru.

Dostupnost správců front hostitele tématu, kteří používají směrování hostitele tématu

V případě směrování hostitelů témat je veškerý systém zpráv publikování/odběru pro téma směrován prostřednictvím správců front, kde je dané téma definováno. Z tohoto důvodu je velmi důležité zvážit nepřetržitou dostupnost těchto správců front v klastru. Pokud se hostitel tématu stane nedostupným a pro dané téma neexistuje žádný jiný hostitel, dojde k okamžitému zastavení přenosu z vydavatelů na odběratele v různých správcích front v klastru pro dané téma. Jsou-li k dispozici další hostitelé témat, správci front klastru směrují nový provoz publikování prostřednictvím těchto hostitelů témat a poskytují tak průběžnou dostupnost tras zpráv.

Pokud jde o přímá témata, po 60 dnech, pokud je první hostitel tématu stále nedostupný, je znalost tématu hostitele tématu odebrána z klastru. Jedná-li se o poslední zbývající definici tohoto tématu v klastru, všichni ostatní správci front přestanou předávat publikování libovolnému hostiteli tématu pro směrování.

Chcete-li zajistit odpovídající dostupnost a rozšiřitelnost, je proto vhodné, je-li to možné, definovat každé téma alespoň ve dvou správcích front klastru. To poskytuje ochranu před tím, aby se daný správce front hostitele tématu stal nedostupným. Viz také Vícenásobné definice témat klastru v klastru se směrovaným hostitelem tématu.

Pokud nemůžete konfigurovat více hostitelů témat (například proto, že potřebujete zachovat řazení zpráv) a nemůžete konfigurovat pouze jednoho hostitele témat (protože dostupnost jednoho správce front nesmí ovlivnit tok publikování k odběrům ve všech správcích front v klastru), zvažte konfiguraci tématu jako přímo směrovaného tématu. Tím se vyvarujete závislosti na jednom správci front pro celý klastr, ale stále vyžadujete, aby byl každý jednotlivý správce front k dispozici, aby mohl zpracovávat lokálně hostované odběry a vydavatele.

Blokování klastrovaného publikování/odběru

Zavedení prvního přímo směrovaného klastrovaného tématu do klastru donutí každého správce front v klastru, aby se dozvěděl o všech ostatních správcích front, a potenciálně je přiměje k tomu, aby si navzájem vytvářeli kanály. Pokud to není žádoucí, měli byste místo toho konfigurovat hostitele tématu se směrováním publikování/odběru. Pokud by existence přímo směrovaného klastrovaného tématu mohla ohrozit stabilitu klastru, můžete v důsledku škálování jednotlivých správců front zcela zakázat funkci klastrovaného publikování/odběru nastavením parametru **PSCLUS** na hodnotu `DISABLED` v každém správci front v klastru.

Jak je popsáno v tématu“Přímé směrování v klastrech publikování/odběru” na stránce 74, když zavedete přímo směrované klastrované téma do klastru, všechna dílčí úložiště budou automaticky upozorněna na všechny ostatní členy klastru. Klastrované téma může také vytvořit odběry ve všech ostatních uzlech (například v místech, kde je zadána hodnota **PROXYSUB(FORCE)**) a způsobit spuštění velkého počtu kanálů ze správce front, a to i v případě, že neexistují žádné lokální odběry. Tím se okamžitě načte další zátěž pro každého správce front v klastru. V případě klastru, který obsahuje mnoho správců front, to může vést k významnému snížení výkonu. Proto musí být zavedení přímého směrovaného publikování/odběru klastru pečlivě naplánováno.

Když víte, že klastr nemůže pojmout režijní náklady přímo směrovaného publikování/odběru, můžete místo toho použít téma hostitel směrovaný publikování/odběr. Přehled rozdílů viz “Návrh klastrů publikování/odběru” na stránce 72.

Dáváte-li přednost úplnému zakázání funkcí publikování/odběru pro klastr, můžete tak učinit nastavením atributu správce front **PSCLUS** na hodnotu ZAKÁZÁNO pro každého správce front v klastru. Toto nastavení zakáže v klastru přímé směrování i publikování/odběr směrované hostitelem tématu úpravou tří aspektů funkčnosti správce front:

- Administrátor tohoto správce front již nemůže definovat objekt Topic jako klastrovaný.
- Příchozí definice témat nebo proxy odběry od jiných správců front jsou odmítnuty a je zaprotokolována varovná zpráva informující administrátora o nesprávné konfiguraci.
- Úplná úložiště již automaticky nesdílejí informace o každém správci front se všemi ostatními částečnými úložišti, když obdrží definici tématu.

Ačkoli je parametr **PSCLUS** parametrem každého jednotlivého správce front v klastru, není určen k selektivnímu zakázání publikování/odběru v podmnožině správců front v klastru. Pokud tímto způsobem selektivně zakážete, zobrazí se časté chybové zprávy. Je tomu tak proto, že proxy odběry a definice témat jsou neustále viditelné a odmítnuté, pokud je téma klastrováno ve správci front, kde je povolen produkt **PSCLUS** .

Proto byste měli usilovat o nastavení parametru **PSCLUS** na hodnotu DISABLED v každém správci front v klastru. V praxi však může být obtížné tento stav dosáhnout a udržovat, například správci front se mohou kdykoli připojit ke klastru a opustit jej. Přinejmenším musíte zajistit, aby byl parametr **PSCLUS** ve všech správcích front úplného úložiště nastaven na hodnotu DISABLED . Pokud tak učiníte a ve správci front ENABLED v klastru je následně definováno klastrované téma, nezpůsobí to, že úplná úložiště budou informovat všechny správce front o všech ostatních správcích front, a váš klastr tak bude chráněn před potenciálními problémy s rozšiřováním ve všech správcích front. V tomto scénáři je původ klastrovaného tématu uveden v protokolech chyb správců front úplného úložiště.

Pokud se správce front podílí na jednom či více klastrech publikování/odběru a také na jednom či více klastrech typu point-to-point, musíte pro tohoto správce front nastavit hodnotu **PSCLUS** na hodnotu POVOLENO . Z tohoto důvodu byste při překrývání dvoubodového klastru s klastrem pro publikování a odběr měli v každém klastru použít oddělenou sadu úplných úložišť. Tento přístup umožňuje, aby definice témat a informace o každém správci front proudily pouze v klastru publikování/odběru.

Chcete-li se vyhnout nekonzistentním konfiguracím při změně hodnoty **PSCLUS** z hodnoty ENABLED na hodnotu DISABLED, nemohou v žádném klastru, jehož je tento správce front členem, existovat žádné objekty klastrovaného tématu. Jakákoli taková témata, dokonce i vzdáleně definovaná, musí být odstraněna před změnou **PSCLUS** na DISABLED.

Další informace o příkazu **PSCLUS**viz ALTER QMGR (PSCLUS).

Související pojmy

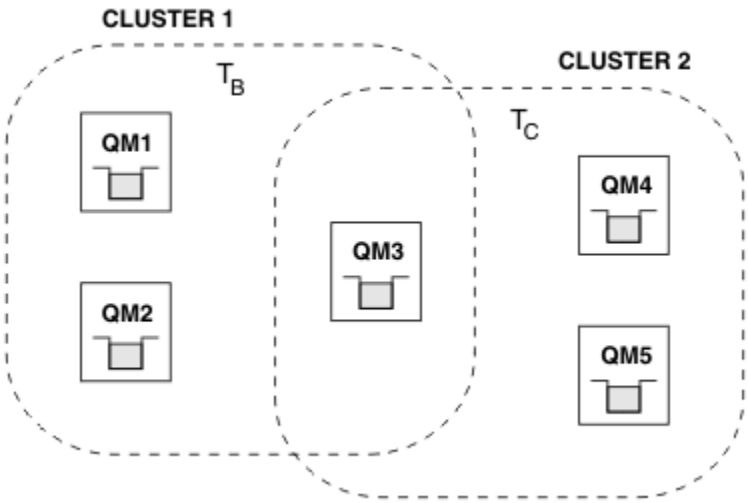
Výkon klastru přímého směrování publikování/odběru

Publikovat/odebírat a více klastrů

Jeden správce front může být členem více než jednoho klastru. Toto uspořádání se někdy nazývá *překrývající se klastry*. Prostřednictvím takového překrytí lze klastrované fronty zpřístupnit z více klastrů a přenos zpráv mezi dvěma body lze směrovat ze správců front v jednom klastru na správce front v jiném klastru. Klastrovaná témata v klastrech publikování/odběru neposkytují stejnou schopnost. Proto musí být jejich chování jasně pochopeno při použití více klastrů.

Na rozdíl od fronty nelze definici tématu přidružit k více než jednomu klastru. Obor klastrovaného tématu je omezen na správce front ve stejném klastru, pro který je téma definováno. To umožňuje šíření publikování na odběry pouze v těch správcích front ve stejném klastru.

Strom témat správce front



Obrázek 28. Překrývající se klastry: Dva klastry, z nichž každý odebírá různá témata

Je-li správce front členem více klastrů, je upozorněn na všechna klastrovaná témata definovaná v každém z těchto klastrů. Například na předchozím obrázku je QM3 informován o spravovaných klastrovaných objektech tématu T_B i $_C$, zatímco QM1 pouze o T_B. QM3 aplikuje obě definice témat na své lokální téma, a proto se u určitých témat chová odlišně od QM1 . Z tohoto důvodu je důležité, aby klastrovaná témata z různých klastrů vzájemně nekolidovaly. K rušení může dojít, když je jedno klastrované téma definováno nad nebo pod jiným klastrovaným tématem v jiném klastru (například mají řetězce tématu `/Sport` a `/Sport/Football`), nebo dokonce pro stejný řetězec tématu v obou. Jinou formou rušení je, když jsou spravované klastrované objekty tématu definovány se stejným názvem objektu v různých klastrech, ale pro různé řetězce témat.

Je-li provedena taková konfigurace, bude doručení publikací do odpovídajících odběrů velmi závislé na relativních umístěních vydavatelů a odběratelů vzhledem ke klastru. Z tohoto důvodu se na takovou konfiguraci nemůžete spolehnout a měli byste ji změnit, abyste odebrali kolidující témata.

Při plánování překrývající se topologie klastru se systémem zpráv publikování/odběru se můžete vyhnout jakémukoli rušení tím, že budete zacházet se stromem témat a názvy objektů klastrovaných témat, jako by pokrývaly všechny překrývající se klastry v topologii.

Integrace více klastrů publikování/odběru

Pokud existuje požadavek na systém zpráv publikování/odběru v různých klastrech, jsou k dispozici dvě možnosti:

- Propojte klastry pomocí konfigurace hierarchie publikování/odběru. Viz Kombinace prostorů témat více klastrů.
- Vytvořte další klastr, který překrývá existující klastry a zahrnuje všechny správce front, kteří potřebují publikovat nebo odebírat konkrétní téma.

S druhou možností byste měli pečlivě zvážit velikost clusteru a nejúčinnější mechanismus směrování clusteru. Viz“Návrh klastrů publikování/odběru” na stránce 72.

Aspekty návrhu pro zachovaná publikování v klastrech publikování/odběru

Při návrhu klastru publikování/odběru pro práci se zachovanými publikacemi je třeba zvážit několik omezení.

Podmínky

Úvaha 1: Následující správci front klastru vždy ukládají nejnovější verzi zachovaného publikování:

- Správce front vydavatele
- V klastru se směrovaným hostitelem tématu se jedná o hostitele tématu (za předpokladu, že pro dané téma existuje pouze jeden hostitel tématu, jak je vysvětleno v další části tohoto článku).
- Všichni správci front s odběry odpovídajícími řetězci tématu zachovaného publikování

2. úvaha: Správci front nepřijímají aktualizovaná zachovaná publikování, pokud nemají žádné odběry. Veškeré zachované publikování uložené ve správci front, který již není přihlášen k odběru tématu, bude proto zastaralé.

Úvaha 3: Pokud při vytváření jakéhokoli odběru existuje lokální kopie zachovaného publikování pro řetězec tématu, je lokální kopie doručena do odběru. Pokud jste prvním odběratelem pro daný řetězec tématu, bude odpovídající zachované publikování doručeno také od jednoho z následujících členů klastru:

- V přímo směrovaném klastru se jedná o správce front vydavatele.
- V klastru se směrovaným hostitelem tématu se jedná o hostitele tématu pro dané téma.

Doručení zachovaného publikování z hostitele tématu nebo správce front publikování do správce front odběru je asynchronní pro volání MQSUB . Proto, pokud použijete volání MQSUBRQ , může být poslední zachované publikování zmeškáno až do následného volání MQSUBRQ.

Důsledky

Pro každý klastr publikování/odběru může při vytvoření prvního odběru lokální správce front ukládat zastaralou kopii zachovaného publikování a toto je kopie, která je doručena novému odběru. Existence odběru v lokálním správci front znamená, že tento problém bude vyřešen při příští aktualizaci zachovaného publikování.

Pokud pro klastr publikování/odběru směrovaný hostitelem tématu konfigurujete pro dané téma více než jednoho hostitele tématu, mohou noví odběratelé obdržet nejnovější zachované publikování od hostitele tématu nebo mohou obdržet zastaralé zachované publikování od jiného hostitele tématu (s tím, že poslední byl ztracen). Pro směrování hostitelů témat je obvyklé konfigurovat pro dané téma více hostitelů témat. Pokud však očekáváte, že aplikace budou používat zachovaná publikování, měli byste pro každé téma nakonfigurovat pouze jednoho hostitele tématu.

Pro každý daný řetězec tématu byste měli použít pouze jednoho vydavatele a zajistit, aby vydavatel vždy používal stejného správce front. Pokud tak neučiníte, mohou být různá zachovaná publikování aktivní v různých správcích front pro stejné téma, což vede k neočekávanému chování. Vzhledem k tomu, že je distribuováno více proxy odběrů, může být přijato více zachovaných publikování.

Máte-li stále obavy o odběratele, kteří používají zastaralá publikování, zvažte nastavení vypršení platnosti zprávy při vytváření jednotlivých zachovaných publikování.

Pomocí příkazu **CLEAR TOPICSTR** můžete odebrat zachované publikování z klastru publikování/odběru. Za určitých okolností může být nutné zadat příkaz pro více členů klastru publikování/odběru, jak je popsáno v tématu **CLEAR TOPICSTR** .

Odběry se zástupnými znaky a zachovaná publikování

Pokud používáte zástupné odběry, odpovídající proxy odběry doručené ostatním členům klastru publikování/odběru jsou bezprostředně před prvním zástupným znakem zástupně odděleny od oddělovače témat. Viz Zástupné znaky a témata klastru.

Proto může použitý zástupný znak odpovídat více řetězcům témat a více zachovaným publikacím, než odpovídá odebírající aplikaci.

Tím se zvýší množství úložného prostoru potřebného pro uchovaná publikování, a proto je třeba zajistit, aby hostitelský správce front měl dostatečnou úložnou kapacitu.

Související pojmy

Zachovaná publikování

Předávání a publikování jednotlivých proxy odběrů všude

Aspekty příkazu REFRESH CLUSTER pro klastry publikování/odběru

Po zadání příkazu **REFRESH CLUSTER** bude správce front dočasně vyřazen lokálně uchovávané informace o klastru, včetně všech témat klastru a jejich přidružených proxy odběrů.

Doba od zadání příkazu **REFRESH CLUSTER** do okamžiku, kdy správce front znovu získá úplné informace o nezbytných informacích pro klastrované publikování/odběr, závisí na velikosti klastru, dostupnosti a schopnosti odezvy správců front úplného úložiště.

Během zpracování aktualizace dochází k přerušení provozu publikování/odběru v klastru publikování/odběru. V případě velkých klastrů může použití příkazu **REFRESH CLUSTER** přerušit probíhající klastr a poté znovu v 27denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zainteresovaným 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 pod vedením centra podpory IBM .

Narušení klastru se může jevit externě jako následující příznaky:

- Odběry témat klastru v tomto správci front nepřijímají publikování od vydavatelů, kteří jsou připojeni k jiným správcům front v klastru.
- Zprávy publikované do témat klastru v tomto správci front nejsou šířeny do odběrů v jiných správcích front.
- Odběry témat klastru v tomto správci front vytvořené během tohoto období neodesílají konzistentně proxy odběry ostatním členům klastru.
- Odběry témat klastru v tomto správci front odstraněné během tohoto období neodebírají konzistentně proxy odběry od ostatních členů klastru.
- 10-sekundové pauzy, nebo delší, při doručování zpráv.
- **MQPUT** selhání, například MQRC_PUBLICATION_FAILURE.
- Publikování umístěná ve frontě nedoručených zpráv s příčinou MQRC_UNKNOWN_REMOTE_Q_MGR

Z těchto důvodů musí být aplikace publikování/odběru uvedeny do klidového stavu před zadáním příkazu **REFRESH CLUSTER** .

Po zadání příkazu **REFRESH CLUSTER** ve správci front v klastru publikování/odběru počkejte na úspěšnou aktualizaci všech správců front klastru a témat klastru a poté znovu synchronizujte proxy odběry podle popisu v části Resynchronizace proxy odběrů. Po správné resynchronizaci všech proxy odběrů restartujte své aplikace publikování/odběru.

Pokud dokončení příkazu **REFRESH CLUSTER** trvá dlouho, monitorujte jej pomocí příkazu CURDEPTH SYSTEM.CLUSTER.COMMAND.QUEUE.

Související pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 66
Pomocí příkazu **REFRESH CLUSTER** vyřadíte všechny lokálně uchovávané informace o klastru a znovu sestavíte tyto informace z úplných úložišť v klastru. Tento příkaz byste neměli používat, s výjimkou výjimečných okolností. Pokud jej potřebujete použít, existují speciální pokyny pro jeho použití. Tyto informace jsou vodítkem na základě testování a zpětné vazby od zákazníků.

Související odkazy

Problémy aplikace při spuštění příkazu REFRESH CLUSTER

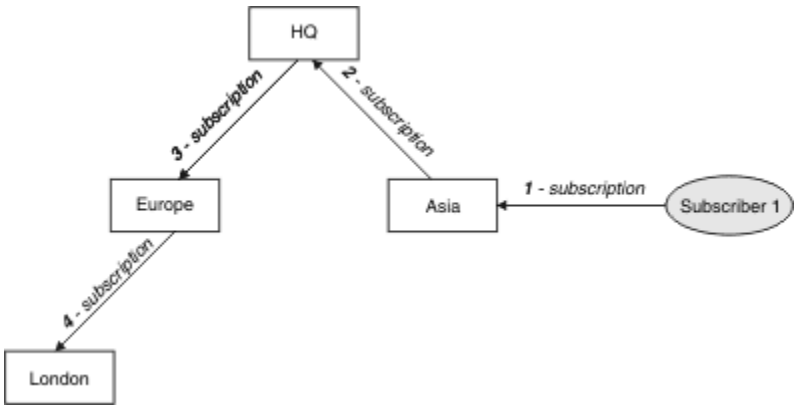
Odkaz na příkazy MQSC: REFRESH CLUSTER

Směrování v hierarchiích publikování/odběru

Pokud je topologie distribuovaného správce front hierarchií publikování/odběru a odběr je proveden ve správci front, bude standardně vytvořen proxy odběr v každém správci front v hierarchii. Publikování přijatá v libovolném správci front jsou poté prostřednictvím hierarchie směrována na všechny správce front, který je hostitelem odpovídajícího odběru.

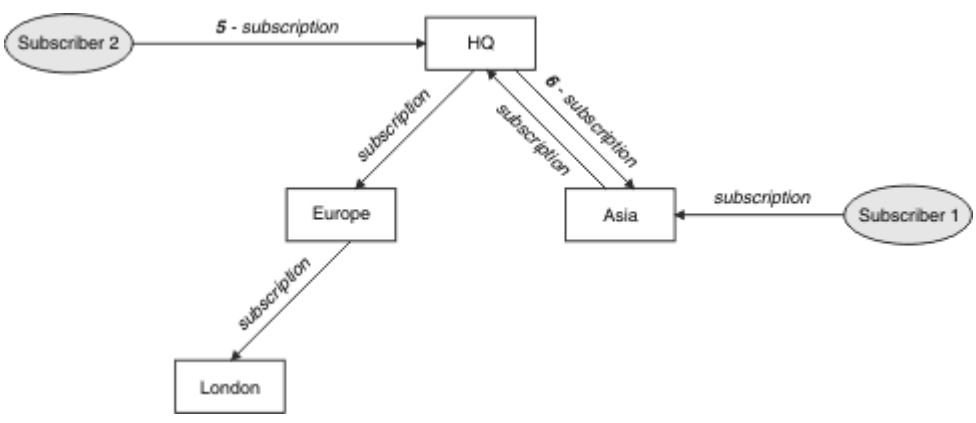
Úvodní informace o směrování zpráv mezi správci front v hierarchiích publikování/odběru a v klastrech naleznete v tématu Distribuované sítě publikování/odběru.

Je-li odběr tématu proveden ve správci front v distribuované hierarchii publikování/odběru, správce front spravuje proces, kterým je odběr šířen do připojených správců front. *Odběry proxy* směřují ke všem správcům front v síti. Proxy odběr poskytuje správci front informace, které potřebuje k předání publikování správcům front, kteří jsou hostiteli odběrů pro dané téma. Každý správce front v hierarchii publikování/odběru si uvědomuje pouze své přímé vztahy. Publikování vložená do jednoho správce front jsou prostřednictvím přímých vztahů odesílána těmto správcům front s odběry. To je ilustrováno na následujícím obrázku, na kterém *Odběratel 1* registruje odběr pro konkrétní téma ve správci front *Asie* (1). Proxy odběry pro tento odběr ve správci front *Asie* jsou předávány všem ostatním správcům front v síti (2,3, 4).



Obrázek 29. Šíření odběrů prostřednictvím sítě správců front

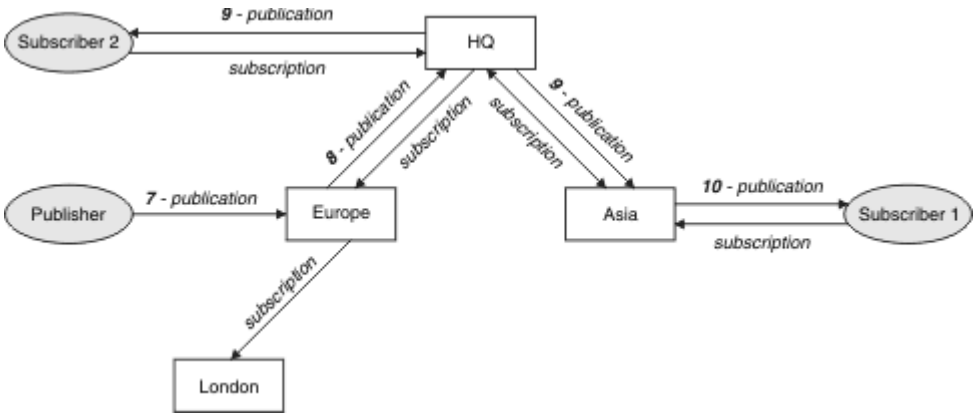
Správce front konsoliduje všechny odběry, které jsou v něm vytvořeny, ať už z lokálních aplikací nebo ze vzdálených správců front. Vytvoří proxy odběry pro témata odběrů se svými sousedy, pokud proxy odběr již neexistuje. To je ilustrováno na následujícím obrázku, na kterém *Odběratel 2* registruje odběr ve stejném tématu jako v tématu Obrázek 29 na stránce 103ve správci front *HQ* (5). Odběr pro toto téma je předán správci front *Asie* , takže si je vědom toho, že odběry existují jinde v síti (6). Odběr není předán správci front *Europe* , protože odběr pro toto téma již byl registrován; viz krok 3 v části Obrázek 29 na stránce 103.



Obrázek 30. Více odběrů

Když aplikace publikuje informace do tématu, přijímající správce front je standardně předá všem správcům front, kteří mají platné odběry tématu. Může ji předávat prostřednictvím jednoho nebo více intermediačních správců front. To je ilustrováno na následujícím obrázku, na kterém vydavatel odešle publikaci ve stejném tématu jako v tématu Obrázek 30 na stránce 103správci front *Evropa* (7). Odběr pro toto téma existuje z *HQ* do *Evropy*, takže publikace je předána správci front *HQ* (8). Z *Londýna* do *Europe* však neexistuje žádný odběr (pouze z *Europe* do *London*), takže publikace není předána správci front

London . Správce front *HQ* odešle publikování přímo do *Odběratel 2* a do správce front *Asie* (9). Publikace je předána *Odběrateli 1* z *Asie* (10).



Obrázek 31. Šíření publikací prostřednictvím sítě správců front

Když správce front odešle publikování nebo odběry jinému správci front, nastaví ve zprávě své vlastní ID uživatele. Používáte-li hierarchii publikování/odběru a je-li příchozí kanál nastaven tak, aby do zprávy vkládal zprávy s oprávněním ID uživatele, musíte autorizovat ID uživatele odesílajícího správce front. Viz Použití výchozích ID uživatelů s hierarchií správce front.

Poznámka: Pokud místo toho použijete klastry publikování/odběru, bude autorizace zpracována klastrem.

Souhrn a další aspekty

Hierarchie publikování/odběru vám poskytuje přesnou kontrolu nad vztahem mezi správci front. Poté, co byl vytvořen, potřebuje malý ruční zásah spravovat. Nicméně to také ukládá určitá omezení na vašem systému:

- Vyšší uzly v hierarchii, zejména kořenový uzel, musí být hostovány na robustním, vysoce dostupném a výkonném vybavení. Důvodem je skutečnost, že se očekává, že těmito uzly projde více publikačního provozu.
- Dostupnost všech nekoncových správců front v hierarchii ovlivňuje schopnost sítě směňovat zprávy od vydavatelů k odběratelům v jiných správcích front.
- Standardně jsou všechny odebírané řetězce témat šířeny v rámci hierarchie a publikování jsou šířena pouze do vzdálených správců front, kteří mají odběr přidruženého tématu. Proto se rychlé změny v sadě odběrů mohou stát limitujícím faktorem. Toto výchozí chování můžete změnit a místo toho můžete všechna publikování šířit do všech správců front, což odebere potřebu proxy odběrů. Viz Výkon odběru v sítích publikování/odběru.

  Poznámka: Podobné omezení platí i pro přímo směrované klastry.
- Vzhledem k vzájemně provázané povaze správců front publikování/odběru trvá, než se proxy odběry rozšíří kolem všech uzlů v síti. Vzdálená publikování nemusí být nutně okamžitě přihlášena k odběru, takže po přihlášení k odběru nového řetězce tématu nemusí být odeslána časná publikování. Problémy způsobené prodlevou odběru můžete odebrat tak, že všechny publikace budou šířeny do všech správců front, což odstraní potřebu proxy odběrů. Viz Výkon odběru v sítích publikování/odběru.

  Poznámka: Toto omezení platí také pro přímo směrované klastry.
- V případě hierarchie publikování/odběru vyžaduje přidání nebo odebrání správců front ruční konfiguraci hierarchie s pečlivým zohledněním umístění těchto správců front a jejich závislosti na jiných správcích front. Pokud nepřidáváte nebo neodebíráte správce front, kteří jsou ve spodní části hierarchie, a proto pod nimi nejsou žádné další větve, budete muset v hierarchii také nakonfigurovat další správce front.

Než použijete hierarchii publikování/odběru jako mechanizmus směrování, prozkoumejte alternativní přístupy, které jsou podrobně popsány v části “Přímé směrování v klastrech publikování/odběru” na stránce 74 a “Směrování hostitelů témat v klastrech publikování/odběru” na stránce 79.

Systémové fronty distribuovaného publikování/odběru

Správci front používají pro systém zpráv publikování/odběru čtyři systémové fronty. Musíte si být vědomi jejich existence pouze pro účely určování problémů a plánování kapacity.

Pokyny k monitorování těchto front naleznete v tématu Vyvažování producentů a spotřebitelů v sítích publikování/odběru .

Tabulka 6. Systémové fronty publikování/odběru na platformě Multiplatforms

Systémová fronta	**Účel**
SYSTEM.INTER.QMGR.CONTROL	IBM MQ distribuovaná řídicí fronta publikování/odběru
SYSTEM.INTER.QMGR.FANREQ	IBM MQ distribuovaná vstupní fronta procesu výstupního větvení serveru proxy pro publikování/odběr
SYSTEM.INTER.QMGR.PUBS	IBM MQ distribuované publikování/odběr publikování
SYSTEM.HIERARCHY.STATE	IBM MQ stav vztahu distribuované hierarchie publikování/odběru

z/OS V systému z/OSnastavíte nezbytné systémové objekty při vytváření správce front zahrnutím ukázek CSQ4INSX, CSQ4INSR a CSQ4INSG do datové sady vstupu inicializace CSQINP2 . Další informace viz Úloha 13: Přizpůsobení vstupních datových sad inicializace.

Atributy front systému publikování/odběru jsou zobrazeny v souboru Tabulka 7 na stránce 105.

Tabulka 7. Atributy systémových front publikování/odběru

Atribut	**Výchozí hodnota**
DEFPSIST	Ano
DEFSOPT	SHARED
MAXMSGL	Multi V systému Multiplatforms: Hodnota parametru MAXMSGL příkazu ALTER QMGR z/OS Na systému z/OS: 4194304 (tj. 4 MB)
MAXDEPTH	999999999
SHARE	Není k dispozici
z/OS z/OS STGCLASS	Tento atribut se používá pouze na platformách z/OS

Poznámka: Jedinou frontou, která obsahuje zprávy vkládané aplikacemi, je fronta `SYSTEM.INTER.QMGR.PUBS`. Parametr **MAXDEPTH** je nastaven na maximální hodnotu pro tuto frontu, aby umožňoval dočasné sestavení publikovaných zpráv během výpadků nebo v době nadměrného zatížení. Je-li správce front spuštěn v systému, v němž nebyla tato hloubka fronty obsažena, je třeba tuto hodnotu upravit.

Související úlohy

Odstraňování problémů s distribuovaným publikováním/odběry

Chyby systémové fronty distribuovaného publikování/odběru

K chybám může dojít v případě, že nejsou k dispozici distribuované fronty správce front publikování/odběru. To má vliv na šíření znalostí odběrů v rámci sítě publikování/odběru a publikování do odběrů ve vzdálených správcích front.

Není-li fronta požadavků výstupního větvení `SYSTEM.INTER.QMGR.FANREQ` k dispozici, může vytvoření odběru generovat chybu a chybové zprávy budou zapsány do protokolu chyb správce front v případě, že proxy odběry musí být doručeny přímo připojeným správcům front.

Není-li fronta stavu vztahu hierarchie `SYSTEM.HIERARCHY.STATE` k dispozici, do protokolu chyb správce front se zapíše chybová zpráva a stroj publikování/odběru se přepne do režimu `COMPAT` . Chcete-li zobrazit režim publikování/odběru, použijte příkaz `DISPLAY QMGR PSMODE`.

Pokud nejsou k dispozici žádné jiné fronty `SYSTEM.INTER.QMGR` , do protokolu chyb správce front se zapíše chybová zpráva, a ačkoli funkce není zakázána, je pravděpodobné, že se zprávy publikování/odběru budou sestavovat ve frontách na tomto nebo vzdálených správcích front.

Pokud není k dispozici systémová fronta publikování/odběru nebo požadovaná přenosová fronta pro nadřízeného, podřízeného nebo podřízeného správce front klastru publikování/odběru, dojde k následujícím výsledkům:

- Publikace nejsou doručeny a aplikace publikování může obdržet chybu. Podrobnosti o době, kdy publikační aplikace obdrží chybu, naleznete v následujících parametrech příkazu **`DEFINE TOPIC`** : **`PMSGDLV`** , **`NPMSGDLV`** a **`USEDLQ`** .
- Přijatá publikování mezi správci front jsou zálohována do vstupní fronty a následně znovu vyzkoušena. Je-li dosažena prahová hodnota vrácení, nedoručená publikování se umístí do fronty nedoručených zpráv. Podrobnosti o problému budou uvedeny v protokolu chyb správce front.
- Nedoručený proxy odběr je odvolán do fronty požadavků na výstupní větvení a následně znovu proveden pokus o jeho provedení. Je-li dosaženo prahové hodnoty vrácení, nedoručený proxy odběr nebude doručen žádnému připojenému správci front a bude umístěn do fronty nedoručených zpráv. Protokol chyb správce front bude obsahovat podrobnosti o problému, včetně podrobností o nezbytných nápravných administrativních akcích.
- Zprávy protokolu relace hierarchie se nezdaří a stav připojení je označen jako ERROR. Chcete-li zobrazit stav připojení, použijte příkaz **`DISPLAY PUBSUB`**.

Související úlohy

Odstraňování problémů s distribuovaným publikováním/odběry

Multi Plánování požadavků na úložiště a výkon na platformě Multiplatforms

Musíte nastavit realistické a dosažitelné úložiště a výkonnostní cíle pro systém IBM MQ . Pomocí odkazů zjistíte faktory, které ovlivňují úložiště a výkon na vaší platformě.

Požadavky se liší v závislosti na systémech, na kterých používáte produkt IBM MQ , a na tom, jaké komponenty chcete použít.

Nejnovější informace o podporovaných hardwarových a softwarových prostředích viz Systémové požadavky pro IBM MQ.

Produkt IBM MQ ukládá data správce front do systému souborů. Pomocí následujících odkazů zjistíte informace o plánování a konfiguraci adresářových struktur pro použití s produktem IBM MQ:

- “Plánování podpory systému souborů na platformě Multiplatforms” na stránce 111
- “Požadavky na sdílené systémy souborů na platformě Multiplatforms” na stránce 112
- “Sdílení souborů IBM MQ na platformě Multiplatforms” na stránce 121
- Linux AIX “Adresářová struktura na systémech AIX and Linux” na stránce 123
- Windows “Adresářová struktura na systémech Windows” na stránce 132

- IBM i "Adresářová struktura na systému IBM i" na stránce 136

Pomocí následujících odkazů získáte informace o systémových prostředcích, sdílené paměti a prioritě procesu v systému AIX and Linux:

- Linux AIX "Prostředky IBM MQ a UNIX System V IPC" na stránce 140
- AIX "Sdílená paměť v systému AIX" na stránce 139
- Linux AIX "IBM MQ a UNIX Priorita procesu" na stránce 140

Chcete-li získat informace o souborech protokolu, použijte následující odkazy:

- "Volba kruhového nebo lineárního protokolování na platformě Multiplatforms" na stránce 139
- Výpočet velikosti protokolu

Související pojmy

"Plánování prostředí IBM MQ na systému z/OS" na stránce 140
Při plánování prostředí IBM MQ musíte vzít v úvahu požadavky na prostředky pro datové sady, sady stránek, Db2, zařízení Coupling Facilities a prostředky pro protokolování a zálohování. Toto téma použijte k plánování prostředí, kde je spuštěn produkt IBM MQ .

Související úlohy

"Plánování architektury IBM MQ" na stránce 5
Při plánování prostředí IBM MQ zvažte podporu, kterou produkt IBM MQ poskytuje pro jednu a více architektur správců front a pro styly systému zpráv typu point-to-point a publikování/odběr. Také naplánujte své požadavky na prostředky a použití protokolovacích a zálohovacích zařízení.

Související odkazy

Hardwarové a softwarové požadavky na AIX and Linux
Hardwarové a softwarové požadavky na Windows

Multi Požadavky na místo na disku na platformě Multiplatforms

Požadavky na úložiště pro produkt IBM MQ závisí na tom, které komponenty instalujete a kolik pracovního prostoru potřebujete.

Diskové úložiště je vyžadováno pro volitelné komponenty, které jste zvolili k instalaci, včetně všech nezbytných komponent, které vyžadují. Celkový požadavek na úložiště také závisí na počtu front, které používáte, počtu a velikosti zpráv ve frontách a na tom, zda jsou zprávy trvalé. Také potřebujete archivační kapacitu na disku, pásce nebo jiném médiu, stejně jako prostor pro vlastní aplikační programy.

Následující tabulky uvádějí přibližný prostor na disku požadovaný při instalaci různých kombinací produktu na různých platformách. (Hodnoty jsou zaokrouhleny nahoru na nejbližší 5 MB, kde MB je 1 048 576 bajtů.)

- LTS "Požadavky na místo na disku pro Long Term Support" na stránce 107
- CD "Požadavky na místo na disku pro Continuous Delivery" na stránce 108

Požadavky na místo na disku pro Long Term Support

LTS V 9.3.0

Tabulka 8. IBM MQ požadavky na místo na disku pro produkt Multiplatforms for Long Term Support

Platforma	Instalace klienta "1" na stránce 108	Instalace serveru "2" na stránce 108	Úplná instalace "3" na stránce 108
AIX AIX	335 MB	375 MB	1810 MB

Tabulka 8. IBM MQ požadavky na místo na disku pro produkt Multiplatforms for Long Term Support (pokračování)			
Platforma	**Instalace klienta** “1” na stránce 108	**Instalace serveru** “2” na stránce 108	**Úplná instalace** “3” na stránce 108
IBM i IBM i (viz Další poznámky k systému IBM i)	485 MB	845 MB	1965 MB
Linux Linux for x86-64	270 MB	295 MB	2010 MB
Linux Linux on Power Systems - Little Endian	170 MB	190 MB	1400 MB
Linux Linux for IBM Z	255 MB	290 MB	1485 MB
Windows Windows (64bitová instalace) “4” na stránce 108	295 MB	415 MB	2310 MB

Notes:

1. Instalace klienta zahrnuje následující komponenty:
   - Běhové prostředí
   - Klient
2. Instalace serveru zahrnuje následující komponenty:
   - Běhové prostředí
   - Server
3. Úplná instalace zahrnuje všechny dostupné komponenty.
4. Windows Ne všechny zde uvedené komponenty jsou instalovatelné funkce na systémech Windows ; jejich funkčnost je někdy zahrnuta v jiných funkcích. Viz IBM MQ funkce pro Windows systémy.

Další poznámky k systému IBM i: IBM i

1. V systému IBM i nemůžete oddělit nativního klienta od serveru. Obrázek serveru v tabulce je pro 5724H72*BASE bez Java, společně s anglickou jazykovou zátěží (2924). K dispozici je 22 možných jedinečných jazykových zátěží.
2. Obrázek v tabulce je pro nativního klienta 5725A49 *BASE without Java.
3. Třídy Java a JMS lze přidat do vazeb serveru i klienta. Chcete-li zahrnout tyto funkce, přidejte 110 MB.
4. Přidání zdroje ukázek do klienta nebo serveru přidá dalších 10 MB.
5. Přidání ukázek do tříd Java a JMS přidá dalších 5 MB.

Požadavky na místo na disku pro Continuous Delivery

V 9.3.0 CD

Tabulka 9. IBM MQ požadavky na místo na disku pro produkt Multiplatforms for Continuous Delivery			
Platforma/CD vydání	**Instalace klienta** "1" na stránce 110	**Instalace serveru**"2" na stránce 111	**Úplná instalace** "3" na stránce 111
AIX **AIX**			
V 9.3.0 IBM MQ 9.3.0	330 MB	375 MB	1760 MB
V 9.3.1 IBM MQ 9.3.1	340 MB	375 MB	1815 MB
V 9.3.2 IBM MQ 9.3.2	355 MB	390 MB	1440 MB
V 9.3.3 IBM MQ 9.3.3	355 MB	390 MB	1440 MB
V 9.3.4 IBM MQ 9.3.4	355 MB	390 MB	1440 MB
V 9.3.5 IBM MQ 9.3.5	355 MB	390 MB	1440 MB
Linux **Linux pro x86-64 (64bitový)**			
V 9.3.0 IBM MQ 9.3.0	265 MB	295 MB	2010 MB
V 9.3.1 IBM MQ 9.3.1	275 MB	295 MB	2010 MB
V 9.3.2 IBM MQ 9.3.2	280 MB	295 MB	1195 MB
V 9.3.3 IBM MQ 9.3.3	280 MB	295 MB	1195 MB
V 9.3.4 IBM MQ 9.3.4	280 MB	295 MB	1195 MB
V 9.3.5 IBM MQ 9.3.5	280 MB	295 MB	1195 MB
Linux **Linux on Power Systems - Little Endian**			
V 9.3.0 IBM MQ 9.3.0	170 MB	190 MB	1350 MB
V 9.3.1 IBM MQ 9.3.1	170 MB	195 MB	1400 MB
V 9.3.2 IBM MQ 9.3.2	170 MB	195 MB	1075 MB

Tabulka 9. IBM MQ požadavky na místo na disku pro produkt Multiplatforms for Continuous Delivery (pokračování)

Platforma/CD vydání	Instalace klienta "1" na stránce 110	Instalace serveru "2" na stránce 111	Úplná instalace "3" na stránce 111
V 9.3.3 IBM MQ 9.3.3	170 MB	195 MB	1075 MB
V 9.3.4 IBM MQ 9.3.4	170 MB	195 MB	1075 MB
V 9.3.5 IBM MQ 9.3.5	170 MB	195 MB	1075 MB
Linux **Linux pro IBM Z**			
V 9.3.0 IBM MQ 9.3.0	255 MB	290 MB	1435 MB
V 9.3.1 IBM MQ 9.3.1	255 MB	290 MB	1485 MB
V 9.3.2 IBM MQ 9.3.2	260 MB	290 MB	1160 MB
V 9.3.3 IBM MQ 9.3.3	260 MB	290 MB	1160 MB
V 9.3.4 IBM MQ 9.3.4	260 MB	290 MB	1160 MB
V 9.3.5 IBM MQ 9.3.5	260 MB	290 MB	1160 MB
Windows **Windows (64bitová instalace)** "4" na stránce 111			
V 9.3.0 IBM MQ 9.3.0	290 MB	410 MB	2095 MB
V 9.3.1 IBM MQ 9.3.1	295 MB	415 MB	2310 MB
V 9.3.2 IBM MQ 9.3.2	300 MB	415 MB	1785 MB
V 9.3.3 IBM MQ 9.3.3	300 MB	415 MB	1785 MB
V 9.3.4 IBM MQ 9.3.4	300 MB	415 MB	1785 MB
V 9.3.5 IBM MQ 9.3.5	300 MB	415 MB	1785 MB

Notes:

1. Instalace klienta zahrnuje následující komponenty:

- Běhové prostředí
- Klient

2. Instalace serveru zahrnuje následující komponenty:
   - Běhové prostředí
   - Server
3. Úplná instalace zahrnuje všechny dostupné komponenty.
4. Windows Ne všechny zde uvedené komponenty jsou instalovatelné funkce na systémech Windows ; jejich funkčnost je někdy zahrnuta v jiných funkcích. Viz IBM MQ funkce pro Windows systémy.

Související pojmy
Funkce a komponenty IBM MQ

Multi Plánování podpory systému souborů na platformě Multiplatforms

Data správce front jsou uložena v systému souborů. Správce front používá zamykání systému souborů, aby zabránil aktivování více instancí správce front s více instancemi současně.

Sdílené systémy souborů

Sdílené systémy souborů umožňují více systémům souběžný přístup ke stejnému fyzickému úložnému zařízení. K poškození by došlo, pokud by více systémů přistupovalo ke stejnému fyzickému úložnému zařízení přímo bez použití prostředků pro vynucení zamykání a řízení souběžnosti. Operační systémy poskytují lokální systémy souborů s uzamykáním a řízením souběžnosti pro lokální procesy; síťové systémy souborů zajišťují uzamykání a řízení souběžnosti pro distribuované systémy.

Historicky nebyly síťové systémy souborů provedeny dostatečně rychle nebo poskytovaly dostatečné zamykání a řízení souběžnosti, aby splňovaly požadavky na protokolování zpráv. Dnes mohou síťové systémy souborů poskytovat dobrý výkon a implementace spolehlivých protokolů síťového systému souborů, jako např. *RFC 3530, Network File System (NFS) verze 4 protokol*, splňují požadavky na spolehlivé protokolování zpráv.

Sdílené systémy souborů a IBM MQ

Data správce front pro správce front s více instancemi jsou uložena ve sdíleném síťovém systému souborů. V systémech AIX, Linux, and Windows musí být datové soubory a soubory protokolu správce front umístěny ve sdíleném síťovém systému souborů. IBM i V systému IBM ise místo souborů protokolu používají žurnály a žurnály nelze sdílet. Správci front s více instancemi v systému IBM i používají k zpřístupnění žurnálů mezi různými instancemi správce front replikaci žurnálu nebo přepínatelné žurnály.

Produkt IBM MQ používá zamykání, aby zabránil aktivování více instancí stejného správce front s více instancemi současně. Stejné zamykání také zajišťuje, že dva oddělení správci front nemohou neúmyslně používat stejnou sadu datových souborů správce front. V daném okamžiku může mít zámek pouze jedna instance správce front. V důsledku toho produkt IBM MQ podporuje data správce front uložená v síťovém úložišti, ke kterému je přistupováno jako ke sdílenému systému souborů.

Vzhledem k tomu, že ne všechny uzamykací protokoly síťových systémů souborů jsou robustní a systém souborů může být konfigurován pro výkon spíše než pro integritu dat, musíte spustit příkaz **amqmfsck** a otestovat, zda síťový systém souborů bude správně řídit přístup k datům a protokolům správce front. Tento příkaz platí pouze pro systémy UNIX, Linux a IBM i . V systému Windowsexistuje pouze jeden podporovaný síťový systém souborů a příkaz **amqmfsck** není povinný.

Související úlohy
“Ověření chování sdíleného systému souborů na platformě Multiplatforms” na stránce 113
Spuštěním příkazu **amqmfsck** zkontrolujte, zda sdílený systém souborů v systémech AIX, Linux nebo IBM i splňuje požadavky na ukládání dat správce front pro správce front s více instancemi. (Jediný požadavek na konfiguraci systému Windows je, že používá SMB 3 pro zajištění sdíleného úložiště.)

Multi Požadavky na sdílené systémy souborů na platformě Multiplatforms

Sdílené systémy souborů musí poskytovat integritu zápisu dat, zaručovat výlučný přístup k souborům a uvolňovat zámky při selhání spolehlivé práce s produktem IBM MQ.

Požadavky, které musí sdílený systém souborů splňovat

Existují tři základní požadavky, které musí sdílený systém souborů splňovat, aby mohl spolehlivě pracovat s produktem IBM MQ:

1. Integrita zápisu dat

   Integrita zápisu dat se někdy nazývá *Zapsat na disk při vyprázdnění*. Správce front musí být schopen provést synchronizaci s daty, která byla úspěšně potvrzena pro fyzické zařízení. V transakčním systému si musíte být jisti, že některé zápisy byly bezpečně potvrzeny, než budete pokračovat v dalším zpracování.

   Konkrétně platformy IBM MQ for AIX or Linux používají volbu otevření *O_SYNC* a systémové volání `fsync()` k explicitnímu vynucení zápisu na obnovitelná média a operace zápisu závisí na správném fungování těchto voleb.

   Upozornění: Linux Systém souborů byste měli připojit pomocí volby `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 i nadále exportovat systém souborů pomocí volby `sync` .

2. Zaručený exkluzivní přístup k souborům

   Chcete-li synchronizovat více správců front, je třeba, aby existoval mechanizmus správce front pro získání výlučného zámku na souboru.

3. Uvolnit zámky při selhání

   Pokud dojde k selhání správce front nebo k selhání komunikace se systémem souborů, je třeba soubory uzamčené správcem front odemknout a zpřístupnit ostatním procesům bez čekání na opětovné připojení správce front k systému souborů.

Sdílený systém souborů musí splňovat tyto požadavky, aby produkt IBM MQ fungoval spolehlivě. V opačném případě dojde k poškození dat a protokolů správce front při použití sdíleného systému souborů v konfiguraci správce front s více instancemi.

V případě správců front s více instancemi v systému Microsoft Windowsmusí k síťovému úložišti přistupovat protokol SMB (Server Message Block) používaný sítěmi Microsoft Windows . Klient SMB (Server Message Block) nesplňuje požadavky IBM MQ na zamykání sémantiky na jiných platformách než Microsoft Windows, takže správci front s více instancemi běžící na jiných platformách než Microsoft Windows nesmí používat SMB (Server Message Block) jako svůj sdílený systém souborů.

V případě správců front s více instancemi na jiných podporovaných platformách musí být k úložišti přistupováno pomocí protokolu síťového systému souborů, který vyhovuje standardu Posix a podporuje zamykání na základě pronájmu. Síťový systém souborů 4 splňuje tento požadavek. Starší systémy souborů, například síťový systém souborů verze 3, které nemají spolehlivý mechanismus pro uvolnění zámků po selhání, nesmí být používány se správci 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 nakonfigurován pro spolehlivost. Sdílené systémy souborů někdy poskytují volby konfigurace ke zvýšení výkonu na úkor spolehlivosti.

Další informace naleznete v tématu Testování příkazu pro IBM MQ systémy souborů správce front s více instancemi.

Za normálních okolností IBM MQ pracuje správně s ukládáním atributů do mezipaměti a není nutné ukládání do mezipaměti zakázat, například nastavením NOAC na připojení NFS . Ukládání atributů do mezipaměti 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 používané každým klientem nemusí být stejné jako tyto atributy na serveru. Příkladem souborů, k nimž je přistupováno tímto způsobem, jsou protokoly chyb správce front pro správce front s více instancemi. Protokoly chyb správce front mohou být zapsány aktivní i rezervní instancí správce front a atributy souborů uložených v mezipaměti mohou způsobit, že protokoly chyb budou větší, než se očekávalo, než dojde k jejich přetočení.

Chcete-li pomoci zkontrolovat systém souborů, spusťte úlohu Ověření chování sdíleného systému souborů. Tato úloha zkontroluje, zda sdílený systém souborů splňuje požadavky 2 a 3. Je třeba ověřit požadavek 1 v dokumentaci sdíleného systému souborů nebo experimentovat s protokolováním dat na disk.

Poruchy disku mohou způsobit chyby při zápisu na disk, což produkt IBM MQ vykazuje jako chyby komponenty First Failure Data Capture. Můžete spustit kontrolu systému souborů pro váš operační systém, abyste zkontrolovali, zda sdílený systém souborů neobsahuje jakékoli poruchy disku. Příklad:

- Linux AIX V systému AIX and Linux se kontrola systému souborů nazývá fsck.
- Windows Na platformách Windows se kontrola systému souborů nazývá CHKDSK nebo SCANDISK.

Zabezpečení serveru NFS

Notes:

- Nemůžete použít volby **nosuid** nebo **noexec** pro bod připojení, který se používá k zadržení instalačního adresáře IBM MQ . Důvodem je, že produkt IBM MQ obsahuje spustitelné programy setuid/setgid a nesmí být zabráněno jejich správnému spuštění.
- Pokud umístíte data správce front pouze na server systému souborů NFS (NFS), můžete použít následující tři volby s příkazem připojení, aby byl systém zabezpečený, bez škodlivého dopadu na spuštění správce front:

  noexec
  Pomocí této volby zastavíte spouštění binárních souborů na systému NFS, což zabrání vzdálenému uživateli ve spuštění nežádoucího kódu v systému.

  nosuid
  Pomocí této volby zabráníte použití bitů set-user-identifier a set-group-identifier, které brání vzdálenému uživateli získat vyšší oprávnění.

  nodev
  Pomocí této volby zastavíte použití nebo definování znakových a blokových speciálních zařízení, což zabrání vzdálenému uživateli dostat se z vězení chroot.

IBM i Linux AIX *Ověření chování sdíleného systému souborů na platformě Multiplatforms*

Spuštěním příkazu **amqmfsck** zkontrolujte, zda sdílený systém souborů v systémech AIX, Linux nebo IBM i splňuje požadavky na ukládání dat správce front pro správce front s více instancemi. (Jediný požadavek na konfiguraci systému Windows je, že používá SMB 3 pro zajištění sdíleného úložiště.)

Než začnete

Potřebujete server se síťovým úložištěm a dva další servery, které jsou k němu připojeny a které mají nainstalovaný produkt IBM MQ . Chcete-li konfigurovat systém souborů, musíte mít oprávnění administrátora (root) a musíte být IBM MQ administrátorem pro spuštění **amqmfsck**.

Informace o této úloze

“Požadavky na sdílené systémy souborů na platformě Multiplatforms” na stránce 112 popisuje požadavky na systém souborů pro použití sdíleného systému souborů se správci front s více instancemi. IBM MQ Technická poznámka Příkaz testování pro IBM MQ systémy souborů správce front s více instancemi vypisuje sdílené systémy souborů, se kterými již produkt IBM testoval. Procedura v této úloze popisuje, jak testovat systém souborů, aby vám pomohl posoudit, zda neuvedený systém souborů udržuje integritu dat.

Překonání selhání správce front s více instancemi může být spuštěno selháním hardwaru nebo softwaru, včetně problémů se sítí, které brání správci front v zápisu do jeho dat nebo souborů protokolu. Především máte zájem o způsobení selhání na souborovém serveru. Musíte však také způsobit, že servery IBM MQ selžou a otestují se všechny zámky úspěšně uvolněné. Chcete-li mít jistotu ve sdíleném systému souborů, otestujte všechna následující selhání a všechna další selhání, která jsou specifická pro vaše prostředí:

1. Vypnutí operačního systému na souborovém serveru včetně synchronizace disků.
2. Zastavení operačního systému na souborovém serveru bez synchronizace disků.
3. Stiskněte tlačítko Reset na každém ze serverů.
4. Vytažení síťového kabelu z každého ze serverů.
5. Vytažením napájecího kabelu z každého ze serverů.
6. Vypnutí všech serverů.

Vytvořte adresář v síťovém úložišti, který budete používat ke sdílení dat a protokolů správce front. Vlastníkem adresáře musí být administrátor systému IBM MQ , nebo jinými slovy člen skupiny `mqm` v systému AIX and Linux. Uživatel, který spouští testy, musí mít oprávnění administrátora produktu IBM MQ .

Použijte příklad exportu a připojení systému souborů v tématu Vytvoření správce front s více instancemi v systému Linux nebo Vytvoření správce front s více instancemi pomocí zrcadlení žurnálu a NetServer v systému IBM i , který vám pomůže s konfigurací systému souborů. Různé systémy souborů vyžadují různé kroky konfigurace. Přečtěte si dokumentaci k systému souborů.

Poznámka: Spusťte IBM MQ MQI client ukázkový program **amqsfhac** paralelně s produktem **amqmfsck** , abyste ukázali, že správce front udržuje integritu zpráv během selhání.

Postup

Při každé kontrole zapříčiníte všechna selhání v předchozím seznamu, když je spuštěn kontrolor systému souborů. Pokud hodláte spustit **amqsfhac** ve stejnou dobu jako **amqmfsck**, proveďte úlohu “Spuštění produktu amqsfhac k testování integrity zpráv” na stránce 119 paralelně s touto úlohou.

1. Připojte exportovaný adresář na dva servery IBM MQ .

   Na serveru systému souborů vytvořte sdílený adresář `shared`a podadresář pro uložení dat pro správce front s více instancemi `qmdata`. Příklad nastavení sdíleného adresáře pro správce front s více instancemi v systému Linuxnaleznete v tématu Vytvoření správce front s více instancemi v systému Linux
2. Zkontrolujte základní chování systému souborů.

   Na jednom serveru IBM MQ spusťte kontrolu systému souborů bez parametrů.

   Na serveru IBM MQ 1:

   ```
   amqmfsck /shared/qmdata
   ```
3. Zkontrolujte souběžné zapisování do stejného adresáře z obou serverů IBM MQ .

   Na obou serverech IBM MQ spusťte kontrolu systému souborů současně s volbou `-c` .

Na serveru IBM MQ 1:

```
amqmfsck -c /shared/qmdata
```

Na serveru IBM MQ 2:

```
amqmfsck -c /shared/qmdata
```

4. Zkontrolujte čekání a uvolnění zámků na obou serverech IBM MQ .
   Na obou serverech IBM MQ spusťte kontrolu systému souborů současně s volbou `-w` .

   Na serveru IBM MQ 1:

   ```
   amqmfsck -w /shared/qmdata
   ```

   Na serveru IBM MQ 2:

   ```
   amqmfsck -w /shared/qmdata
   ```

5. Zkontrolujte integritu dat.

   a) Naformátujte testovací soubor.

   Vytvořte v testovaném adresáři velký soubor. Soubor je formátován tak, aby následné fáze mohly být úspěšně dokončeny. Soubor musí být dostatečně velký, aby měl dostatek času na přerušení druhé fáze pro simulaci překonání selhání. Zkuste výchozí hodnotu 262144 stránek (1 GB). Program automaticky sníží tuto předvolbu na pomalých systémech souborů tak, aby se formátování dokončilo přibližně za 60 sekund.

   Na serveru IBM MQ 1:

   ```
   amqmfsck -f /shared/qmdata
   ```

   Server odpoví následujícími zprávami:

   ```
   Formatting test file for data integrity test.

   Test file formatted with 262144 pages of data.
   ```

   b) Zapsat data do testovacího souboru pomocí kontroly systému souborů při způsobení selhání.

   Spusťte testovací program na dvou serverech současně. Spusťte testovací program na serveru, na kterém dojde k selhání, a poté spusťte testovací program na serveru, který selhání přežije. Příčina selhání, které vyšetřujete.

   První testovací program se zastaví s chybovou zprávou. Druhý testovací program získá zámek na testovacím souboru a zapíše data do testovacího souboru počínaje místem, kde první testovací program skončil. Nechte druhý testovací program běžet až do dokončení.

Tabulka 10. Spuštění kontroly integrity dat na dvou serverech současně

IBM MQ server 1	**IBM MQ server 2**
`amqmfsck -a /shared/qmdata`	

Tabulka 10. Spuštění kontroly integrity dat na dvou serverech současně (pokračování)

IBM MQ server 1	**IBM MQ server 2**
	`amqmfsck -a /shared/qmdata`

`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.`
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`

Turn the power off here.	

	`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.`

Časování testu závisí na chování systému souborů. Například obvykle trvá 30-90 sekund, než systém souborů uvolní zámky souborů získané prvním programem po výpadku napájení. Máte-li příliš málo času na zavedení selhání před tím, než první testovací program vyplnil soubor, použijte volbu `-x` **amqmfsck** k odstranění testovacího souboru. Zkuste test od začátku s větším testovacím souborem.

c) Ověřte integritu dat v testovacím souboru.

Na serveru IBM MQ 2:

```
amqmfsck -i /shared/qmdata
```

Server odpoví následujícími zprávami:

```
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.
```

6. Odstraňte testovací soubory.

   Na serveru IBM MQ 2:

```
amqmfsck -x /shared/qmdata
Test files deleted.
```

   Server odpoví zprávou:

```
Test files deleted.
```

Výsledky

Program vrátí nulový kód ukončení, pokud jsou testy úspěšně dokončeny, jinak nenulový.

Příklady

První sada tří příkladů ukazuje příkaz produkující minimální výstup.

Úspěšný test základního zamykání souborů na jednom serveru

```
> amqmfsck /shared/qmdata
The tests on the directory completed successfully.
```

Selhal test základního zamykání souborů na jednom serveru.

```
> amqmfsck /shared/qmdata
AMQ6245: Error Calling 'write()[2]' on file '/shared/qmdata/amqmfsck.lck' error '2'.
```

Úspěšný test zamykání na dvou serverech

Tabulka 11. Úspěšné uzamčení na dvou serverech

IBM MQ server 1	IBM MQ server 2

`> amqmfsck -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.`	

	`> amqmfsck -w /shared/qmdata` `Waiting for lock...`
`[ Return pressed ]` `Lock released.`	

	`Lock acquired.`
	`The tests on the directory completed`
	`successfully`

Druhá sada tří příkladů ukazuje stejné příkazy používající režim s komentářem.

Úspěšný test základního zamykání souborů na jednom serveru

```
> amqmfsck -v /shared/qmdata
System call: stat("/shared/qmdata")'
System call: fd = open("/shared/qmdata/amqmfsck.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/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd1 = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd1, F_SETLK, F_RDLCK)
System call: fd2 = open("/shared/qmdata/amqmfsck.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.
```

Selhal test základního zamykání souborů na jednom serveru.

```
> amqmfsck -v /shared/qmdata
System call: stat("/shared/qmdata")
System call: fd = open("/shared/qmdata/amqmfsck.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/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_RDLCK)
System call: fdSameFile = open("/shared/qmdata/amqmfsck.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/amqmfsck.lck', errno 2
(Permission denied).
```

Úspěšný test zamykání na dvou serverech

Tabulka 12. Úspěšné uzamknutí na dvou serverech-režim s komentářem

IBM MQ server 1	**IBM MQ server 2**

`> amqmfsck -wv /shared/qmdata`
`Calling 'stat("/shared/qmdata")'`
`Calling 'fd = open("/shared/qmdata/`
`amqmfsck.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.`	

	`> amqmfsck -wv /shared/qmdata`
	`Calling 'stat("/shared/qmdata")'`
	`Calling 'fd = open("/shared/qmdata/`
	`amqmfsck.lkw",`
	`O_EXCL | O_CREAT | O_RDWR,0666)'`
	`Calling 'fd = open("/shared/qmdata/amqmfsck.lkw,`
	`O_RDWR, 0666)'`
	`Calling 'fcntl(fd, F_SETLK, F_WRLCK)`
	`'Waiting for lock...`

Tabulka 12. Úspěšné uzamknutí na dvou serverech-režim s komentářem (pokračování)	
IBM MQ server 1	**IBM MQ server 2**

`[ Return pressed ]`
`Calling 'close(fd)'`
`Lock released.`	

	`Calling 'fcntl(fd, F_SETLK, F_WRLCK)'`
	`Lock acquired.`
	`The tests on the directory completed successfully`

Související odkazy

Ukázkové programy s vysokou dostupností

Multi

Spuštění produktu amqsfhac k testování integrity zpráv

Spusťte IBM MQ MQI client ukázkový program **amqsfhac** paralelně s produktem **amqmfsck** , abyste ukázali, že správce front udržuje integritu zpráv během selhání.

Než začnete

Pro tento test potřebujete čtyři servery. Dva servery pro správce front s více instancemi, jeden pro systém souborů a jeden pro spuštění aplikace **amqsfhac** jako IBM MQ MQI client .

Postupujte podle kroku “1” na stránce 114 v části “Ověření chování sdíleného systému souborů na platformě Multiplatforms” na stránce 113 a nastavte systém souborů pro správce front s více instancemi.

Informace o této úloze

IBM MQ MQI client Ukázkový program **amqsfhac** kontroluje, zda správce front používající síťové úložiště udržuje integritu dat po selhání. Spuštěním příkazu **amqsfhac** paralelně s produktem **amqmfsck** můžete demonstrovat, že správce front udržuje integritu zpráv během selhání.

Postup

1. Vytvořte správce front pro více instancí na jiném serveru `QM1`pomocí systému souborů, který jste vytvořili v kroku “1” na stránce 114 v části Procedura.

   Viz Vytvořit správce front s více instancemi.
2. Spusťte správce front na obou serverech, aby byl vysoce dostupný.

   Na serveru 1:

   ```
   strmqm -x QM1
   ```

   Na serveru 2:

   ```
   strmqm -x QM1
   ```
3. Nastavte připojení klienta pro spuštění **amqsfhac**.
   a) Použijte proceduru v části *Ověření IBM MQ instalace* pro platformu nebo platformy, které váš podnik používá k nastavení připojení klienta, nebo vzorové skripty v části Ukázky klienta s možností opětovného připojení.
   b) Upravte kanál klienta tak, aby měl dvě adresy IP odpovídající dvěma serverům se systémem `QM1`.

      V ukázkovém skriptu upravte:

```
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNAME('LOCALHOST(2345)') QMNAME(QM1) REPLACE
```

Komu:

```
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNAME('server1(2345),server2(2345)') QMNAME(QM1) REPLACE
```

kde `server1` a `server2` jsou názvy hostitelů dvou serverů a 2345 je port, na kterém naslouchá modul listener kanálu. Obvykle se použije výchozí hodnota 1414. Produkt 1414 můžete použít s výchozí konfigurací modulu listener.

4. Vytvořte dvě lokální fronty v systému `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. Při testování integrity systému souborů otestujte integritu zpráv.

   Spusťte **amqsfhac** během kroku “5” na stránce 115 z “Ověření chování sdíleného systému souborů na platformě Multiplatforms” na stránce 113.

```
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. Znovu restartujte zastavenou instanci správce front, abyste mohli vrátit selhání v dalším testu. Pravděpodobně budete muset zvýšit počet iterací na základě experimentování s vaším prostředím, aby testovací program běžil dostatečně dlouho, než dojde k překonání selhání.

Výsledky

Příklad spuštění příkazu **amqsfhac** v kroku “6” na stránce 120 je uveden v následujícím příkladu. V tomto příkladu je test úspěšný.

```
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
```

Pokud test zjistil problém, výstup by nahlásil selhání. V některých testovacích bězích `MQRC_CALL_INTERRUPTED` může vykazovat "`Resolving to backed out`". To nic nemění na výsledku. Výsledek závisí na tom, zda byl zápis na disk potvrzen síťovým úložištěm souborů před nebo po selhání.

Související odkazy

amqmfsck (kontrola systému souborů)

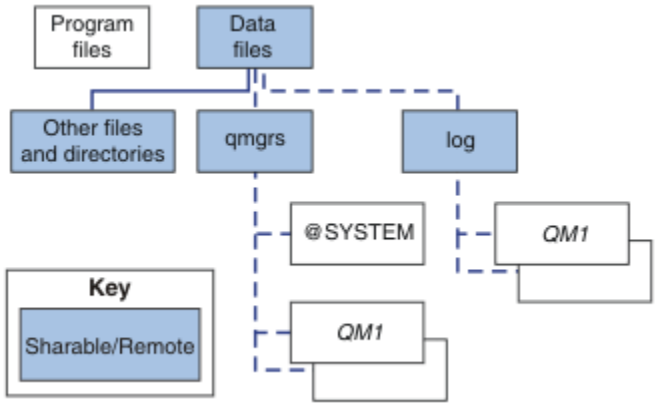
Ukázkové programy s vysokou dostupností

Multi Sdílení souborů IBM MQ na platformě Multiplatforms

K některým souborům IBM MQ přistupuje výhradně aktivní správce front, ostatní soubory jsou sdílené.

Soubory IBM MQ jsou rozděleny do programových souborů a datových souborů. Programové soubory se obvykle instalují lokálně na každý server, na kterém běží produkt IBM MQ. Správci front sdílejí přístup k datovým souborům a adresářům ve výchozím datovém adresáři. Vyžadují výlučný přístup ke svým vlastním adresářovým stromům správce front obsaženým v jednotlivých adresářích `qmgrs` a `log` uvedených v souboru Obrázek 32 na stránce 121.

Obrázek 32 na stránce 121 je vysokoúrovňový pohled na adresářovou strukturu IBM MQ . Zobrazuje adresáře, které lze sdílet mezi správci front a nastavit jako vzdálené. Podrobnosti se liší podle platformy. Tečkované čáry označují konfigurovatelné cesty.



Obrázek 32. Celkový pohled na adresářovou strukturu IBM 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 AIX and Linux a konfigurovatelný při instalaci na systému Windows. Je sdílena mezi správci front. Výchozí umístění můžete nastavit jako vzdálené, ale nesdílejte jej mezi různými instalacemi produktu IBM MQ. Atribut `DefaultPrefix` v konfiguraci IBM MQ ukazuje na tuto cestu.

qmgrs

Existují dva alternativní způsoby určení umístění dat správce front.

Použití atributu Prefix

Atribut **Prefix** určuje umístění adresáře `qmgrs` . Produkt IBM MQ vytvoří název adresáře správce front z názvu správce front a vytvoří jej jako podadresář adresáře `qmgrs` .

Atribut **Prefix** je umístěn v sekci QueueManager souboru `mqs.ini` a je zděděn z hodnoty v atributu **DefaultPrefix** sekce Všichni správci front. Ve výchozím nastavení pro zjednodušení administrace správci front obvykle sdílejí stejný adresář `qmgrs` .

Změníte-li umístění adresáře `qmgrs` pro libovolného správce front, musíte změnit hodnotu jeho atributu **Prefix** .

Atribut **Prefix** pro adresář `QM1` v adresáři Obrázek 32 na stránce 121 pro platformu AIX and Linux je následující:

```
Prefix=/var/mqm
```

Použití atributu DataPath

Atribut **DataPath** určuje umístění datového adresáře správce front.

Atribut **DataPath** určuje úplnou cestu včetně názvu datového adresáře správce front. Atribut **DataPath** se liší od atributu **Prefix** , který určuje neúplnou cestu k datovému adresáři správce front.

Atribut **DataPath** , je-li uveden, je umístěn v sekci QueueManager souboru `mqs.ini` . Pokud byla zadána, má přednost před jakoukoli hodnotou v atributu **Prefix** .

Změníte-li umístění datového adresáře správce front pro libovolného správce front, musíte změnit hodnotu atributu `DataPath` .

Atribut `DataPath` pro adresář `QM1` v adresáři Obrázek 32 na stránce 121pro platformu Linux nebo AIX je následující:

```
DataPath=/var/mqm/qmgrs/QM1
```

log

Adresář protokolu je uveden samostatně pro každého správce front v sekci Log stanza v konfiguraci správce front. Konfigurace správce front je v adresáři `qm.ini`.

Podadresáře *DataPath*/*QmgrName*/@IPCC

Podadresáře *DataPath*/*QmgrName*/`@IPCC` jsou v cestě ke sdílenému adresáři. Používají se k vytvoření cesty k adresáři pro objekty systému souborů IPC. Je-li správce front sdílen mezi systémy, musí rozlišovat obor názvů správce front.

Objekty systému souborů IPC musí být rozlišeny systémem. Do cesty k adresáři je přidán podadresář pro každý systém, ve kterém je spuštěn správce front, viz Obrázek 33 na stránce 122.

```
DataPath/QmgrName/@IPCC/esem/myHostName/
```

Obrázek 33. Příklad podadresáře IPC

myHostName je až prvních 20 znaků názvu hostitele vráceného operačním systémem. Na některých systémech může být název hostitele až 64 znaků dlouhý před oříznutím. Generovaná hodnota *myHostName* může způsobit problém ze dvou příčin:

1. Prvních 20 znaků není jedinečných.
2. Název hostitele je generován algoritmem DHCP, který systému nepřiděluje vždy stejný název hostitele.

V těchto případech nastavte *myHostName* pomocí proměnné prostředí **MQS_IPC_HOST**; viz Obrázek 34 na stránce 122.

```
export MQS_IPC_HOST= myHostName
```

*Obrázek 34. Příklad: nastavení **MQS_IPC_HOST***

Ostatní soubory a adresáře

Ostatní soubory a adresáře, například adresář obsahující trasovací soubory a společný protokol chyb, jsou obvykle sdíleny a uchovávány v lokálním systému souborů.

S podporou sdílených systémů souborů spravuje produkt IBM MQ výlučný přístup k těmto souborům pomocí zámků systému souborů. Zámek systému souborů umožňuje, aby byla v daném okamžiku aktivní pouze jedna instance konkrétního správce front.

Při spuštění první instance konkrétního správce front převezme vlastnictví svého adresáře správce front. Spustíte-li druhou instanci, může převzít vlastnictví pouze v případě, že byla první instance zastavena. Pokud je první správce front stále spuštěn, druhá instance se nespustí a ohlásí, že je správce front spuštěn jinde. Pokud byl první správce front zastaven, druhý správce front převezme vlastnictví souborů správce front a stane se spuštěným správcem front.

Můžete automatizovat proceduru druhého správce front převzetí od prvního. Spusťte prvního správce front s volbou `strmqm -x` , která povoluje převzetí od jiného správce front. Druhý správce front poté před pokusem o převzetí vlastnictví souborů správce front počká na odemknutí souborů správce front a spustí se.

Linux AIX Adresářová struktura na systémech AIX and Linux

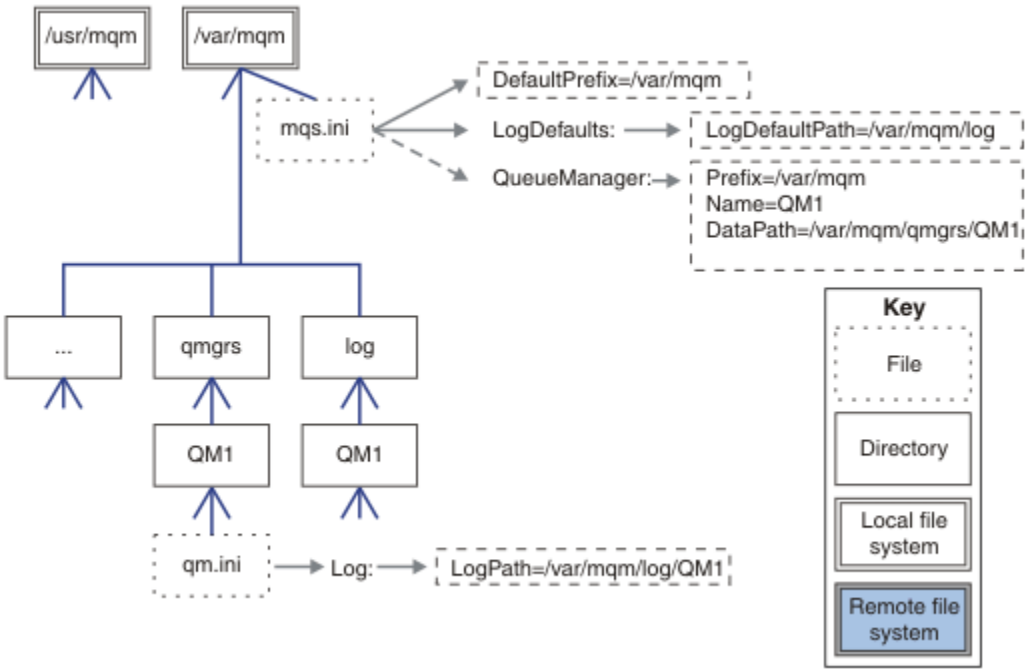
Adresářovou strukturu IBM MQ na systémech AIX and Linux lze mapovat na různé systémy souborů pro snazší správu, lepší výkon a vyšší spolehlivost.

Pomocí flexibilní adresářové struktury produktu IBM MQ můžete využívat výhod sdílených systémů souborů pro spouštění správců front s více instancemi.

Použijte příkaz **crtmqm** *QM1* k vytvoření adresářové struktury zobrazené v Obrázek 35 na stránce 124 , kde R je vydání produktu. Jedná se o typickou adresářovou strukturu pro správce front vytvořeného v systému IBM MQ . Některé adresáře, soubory a nastavení atributů .ini jsou z důvodu přehlednosti vynechány a další název správce front může být změněn manglingem. Názvy systémů souborů se liší v různých systémech.

V typické instalaci se každý správce front, kterého vytvoříte, odkazuje na společné adresáře `log` a `qmgrs` v lokálním systému souborů. V konfiguraci s více instancemi jsou adresáře `log` a `qmgrs` v síťovém systému souborů sdíleném s jinou instalací produktu IBM MQ.

Obrázek 35 na stránce 124 zobrazuje výchozí konfiguraci pro produkt IBM MQ v7.R na AIX , kde R je vydání produktu. Příklady alternativních konfigurací s více instancemi viz“Příklad konfigurací adresáře na systémech AIX and Linux” na stránce 129.



Obrázek 35. Příklad výchozí adresářové struktury IBM MQ pro systémy AIX and Linux

Produkt je standardně nainstalován do adresáře `/usr/mqm` na systému AIX a `/opt/mqm` na ostatních systémech. Pracovní adresáře se instalují do adresáře `/var/mqm` .

Poznámka: Pokud jste vytvořili systém souborů `/var/mqm` před instalací produktu IBM MQ , ujistěte se, že uživatel mqm má úplná oprávnění k adresáři, například souborový režim 755.

Poznámka: Adresář `/var/mqm/errors` by měl být samostatným systémem souborů, aby se zabránilo tomu, že data FFDC vytvořená správcem front zaplní systém souborů, který obsahuje soubor `/var/mqm`.

Další informace viz Vytvoření systémů souborů na AIX and Linux systémech .

Adresáře `log` a `qmgrs` se zobrazí ve výchozích umístěních, jak jsou definována výchozími hodnotami atributů `LogDefaultPath` a `DefaultPrefix` v souboru `mqs.ini` . Při vytvoření správce front je standardně vytvořen datový adresář správce front v adresáři *`DefaultPrefix`*`/qmgrs`a adresář souboru protokolu v adresáři *`LogDefaultPath`*`/log`. `LogDefaultCesta` a `DefaultPrefix` ovlivňuje pouze to, kde jsou standardně vytvářeni správci front a soubory protokolu. Skutečné umístění adresáře správce front je uloženo v souboru `mqs.ini` a umístění adresáře souboru protokolu je uloženo v souboru `qm.ini` .

Adresář souboru protokolu pro správce front je definován v souboru `qm.ini` v atributu `LogPath` . Volbu `-ld` v příkazu **`crtmqm`** použijte k nastavení atributu `LogPath` pro správce front, například **`crtmqm`** `-ld` *`LogPath`* `QM1` . Pokud vynecháte parametr `ld` , použije se místo toho hodnota `LogDefaultPath` .

Datový adresář správce front je definován v atributu `DataPath` v sekci `QueueManager` v souboru `mqs.ini` . Volbu `-md` v příkazu **`crtmqm`** použijte k nastavení `DataPath` pro správce front, například **`crtmqm`** `-md` *`DataPath`* `QM1` . Pokud vynecháte parametr `md` , použije se místo toho hodnota atributu `DefaultPrefix` nebo `Předpona` . `Předpona` má přednost před předponou `DefaultPrefix`.

Obvykle vytvořte `QM1` určující adresář protokolu i datový adresář v jednom příkazu.

```
 crtmqm
-md DataPath -ld
LogPath QM1
```

Umístění protokolu správce front a datových adresářů existujícího správce front můžete upravit úpravou atributů `DataPath` a `LogPath` v souboru `qm.ini` při zastavení správce front.

Cestu k adresáři `errors` , stejně jako cesty ke všem ostatním adresářům v adresáři `/var/mqm`, nelze upravit. Adresáře však mohou být připojeny na různé systémy souborů nebo symbolicky propojeny s různými adresáři.

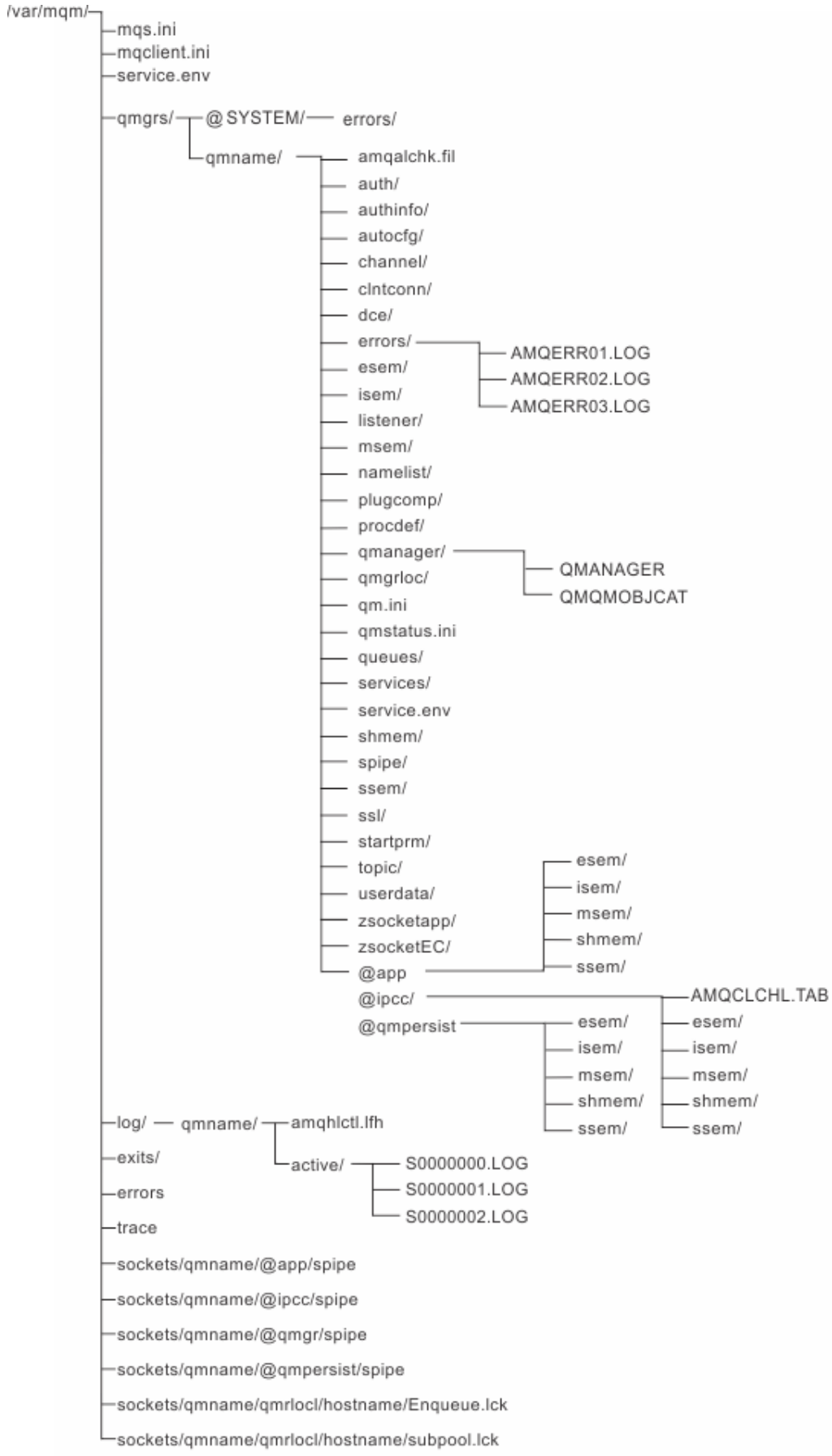
Linux AIX *Obsah adresáře v systémech AIX and Linux*

Obsah adresářů přidružených ke správci front.

Informace o umístění souborů produktu naleznete v tématu Výběr umístění instalace .

Informace o alternativních konfiguracích adresářů viz “Plánování podpory systému souborů na platformě Multiplatforms” na stránce 111.

Následující adresářová struktura je reprezentativní pro produkt IBM MQ poté, co byl správce front po určitou dobu používán. Skutečná struktura, kterou máte, závisí na tom, které operace se ve správci front vyskytly.


/var/mqm/
mqs.ini
mqclient.ini
service.env
qmgrs/
@SYSTEM/
errors/
qmname/
amqalchk.fil
auth/
authinfo/
autocfg/
channel/
clntconn/
dce/
errors/
AMQERR01.LOG
AMQERR02.LOG
AMQERR03.LOG
esem/
isem/
listener/
msem/
namelist/
plugcomp/
procdef/
qmanager/
QMANAGER
QMQMOBJCAT
qmgrloc/
qm.ini
qmstatus.ini
queues/
services/
service.env
shmem/
spipe/
ssem/
ssl/
startprm/
topic/
userdata/
zsocketapp/
zsocketEC/
@app
esem/
isem/
msem/
shmem/
ssem/
@ipcc/
AMQCLCHL.TAB
@qmpersist
esem/
isem/
msem/
shmem/
ssem/
esem/
isem/
msem/
shmem/
ssem/
log/
qmname/
amqhlctl.lfh
active/
S0000000.LOG
S0000001.LOG
S0000002.LOG
exits/
errors
trace
sockets/qmname/@app/spipe
sockets/qmname/@ipcc/spipe
sockets/qmname/@qmgr/spipe
sockets/qmname/@qmpersist/spipe
sockets/qmname/qmrlocl/hostname/Enqueue.lck
sockets/qmname/qmrlocl/hostname/subpool.lck

/var/mqm/

Adresář /var/mqm obsahuje konfigurační soubory a výstupní adresáře, které se vztahují na instalaci produktu IBM MQ jako celek, a nikoli na jednotlivého správce front.

Tabulka 13. Dokumentovaný obsah adresáře /var/mqm na webu AIX and Linux	
Název adresáře nebo souboru	**Obsah**
mqs.ini	Konfigurační soubor pro celou instalaci produktu IBM MQ , načtený při spuštění správce front. Cestu k souboru lze upravit pomocí proměnné prostředí **AMQ_MQS_INI_LOCATION** . Ujistěte se, že je tato volba nastavena a exportována v shellu, ve kterém je spuštěn příkaz **strmqm** .
mqclient.ini	Výchozí konfigurační soubor klienta načtený programy IBM MQ MQI client . Cestu k souboru lze upravit pomocí proměnné prostředí **MQCLNTCF** .
service.env	Obsahuje proměnné prostředí rozsahu počítače pro proces služby. Cesta k souboru byla opravena.
chyby/	Protokoly chyb rozsahu počítače a soubory FFST . Cesta k adresáři byla opravena. Viz také FFST: IBM MQ for UNIX a Linux systémy.
sokety/	Obsahuje informace pro každého správce front pouze pro systémové použití.
trasování/	Trasovací soubory. Cesta k adresáři byla opravena.
web/	Adresář serveru mqweb.
exits/	Výchozí adresář obsahující uživatelské programy uživatelského kanálu. Umístění lze upravit v sekcích ApiExit v souboru mqs.ini .
exits64/	

/var/mqm/qmgrs/*qmname*/

/var/mqm/qmgrs/*qmname*/ obsahuje adresáře a soubory pro správce front. Adresář je uzamčen pro výlučný přístup instance aktivního správce front. Cestu k adresáři lze přímo upravit v souboru mqs.ini nebo pomocí volby **md** příkazu **crtmqm** .

Tabulka 14. Dokumentovaný obsah adresáře /var/mqm/qmgrs/qmname na webu AIX and Linux	
Název adresáře nebo souboru	**Obsah**
qm.ini	Konfigurační soubor správce front, čtení při spuštění správce front.
chyby/	Protokoly chyb oboru správce front. *qmname* = @system obsahuje zprávy související s kanálem pro neznámého nebo nedostupného správce front.

Tabulka 14. Dokumentovaný obsah adresáře /var/mqm/qmgrs/qmname na webu AIX and Linux (pokračování)	
Název adresáře nebo souboru	**Obsah**
@ipcc/ AMQCLCHL.TAB	Výchozí řídicí tabulka kanálu klienta vytvořená serverem IBM MQ a přečtená programy IBM MQ MQI client . Cestu k souboru lze upravit pomocí proměnných prostředí **MQCHLLIB** a **MQCHLTAB** .
QMANAGER	Soubor objektů správce front: QMANAGER Katalog objektů správce front: QMQMOBJCAT
authinfo/	Každý objekt definovaný ve správci front je přidružen k souboru v těchto adresářích. Název souboru přibližně odpovídá názvu definice; viz Základní informace o IBM MQ názvech souborů.
kanál/	
clntconn/(bez připojení)	
modul listener/	
seznam názvů/	
procdef/procdef/	
fronty/	
služby/	
témata/	
...	Ostatní adresáře používané produktem IBM MQ, například @ipcc, které mají být upraveny pouze produktem IBM MQ.
uživatelská data/	Lze použít k uložení trvalého stavu aplikací (může být použit RDQM při přesouvání správců front do různých uzlů-viz Uložení stavu trvalé aplikace.)
DataPath**autocfg	Používá se pro automatickou konfiguraci

/var/mqm/log/*qmname*/

Soubor /var/mqm/log/*qmname*/ obsahuje soubory protokolu správce front. Adresář je uzamčen pro výlučný přístup instance aktivního správce front. Cestu k adresáři lze upravit v souboru qm.ini nebo pomocí volby **ld** příkazu **crtmqm** .

Tabulka 15. Dokumentovaný obsah adresáře /var/mqm/log/qmname na webu AIX and Linux	
Název adresáře nebo souboru	**Obsah**
amqhlctl.lfh	Řídicí soubor protokolu.
aktivní/	Tento adresář obsahuje soubory protokolu s číslem S0000000.LOG, S0000001.LOG, S0000002.LOG, a tak dále.

/opt/mqm

/opt/mqm je standardně instalační adresář na většině platforem. Další informace o velikosti prostoru, který potřebujete pro instalační adresář na platformě nebo platformách, které váš podnik používá, naleznete v části “Požadavky na místo na disku na platformě Multiplatforms” na stránce 107 .

Linux AIX Příklad konfigurací adresáře na systémech AIX and Linux

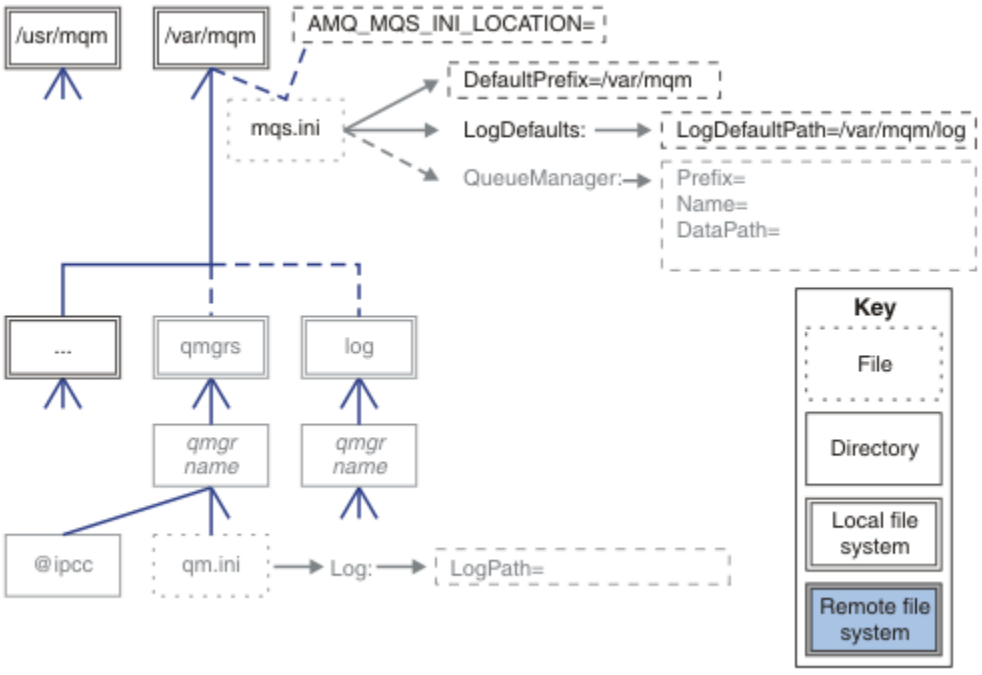
Příklady alternativních konfigurací systému souborů na systémech AIX and Linux .

Adresářovou strukturu IBM MQ můžete upravit různými způsoby, 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 přidělte adresáře různým diskům, abyste zlepšili výkon tím, že snížíte soupeření I/O.
- Použijte rychlejší úložná zařízení pro adresáře, které mají větší vliv na výkon. Latence fyzického zařízení je často důležitějším faktorem ve výkonu trvalého systému zpráv, než zda je zařízení připojeno lokálně nebo vzdáleně. Následující seznam zobrazuje, které adresáře jsou nejvíce a nejméně citlivé na výkon.
  1. `log`
  2. `qmgrs`
  3. Ostatní adresáře, včetně adresáře `/usr/mqm`
- Vytvořte adresáře `qmgrs` a `log` na systémech souborů, které jsou přiděleny k úložišti s dobrou odolností, například redundantní diskové pole.
- Je lepší uložit obecné protokoly chyb v systému `var/mqm/errors`, lokálně, spíše než v síťovém systému souborů, aby bylo možné protokolovat chyby související se síťovým systémem souborů.

Obrázek 36 na stránce 129 je šablona, ze které jsou odvozeny alternativní adresářové struktury IBM MQ . V šabloně tečkované čáry představují cesty, které lze konfigurovat. V příkladech jsou tečkované čáry nahrazeny plnými čarami, 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 objeví v souborech `mqs.ini` nebo `qm.ini` . Zadáte-li v příkazu **crtmqm** parametry cesty, vynechte název adresáře správce front: Název správce front bude přidán do cesty produktem IBM MQ.



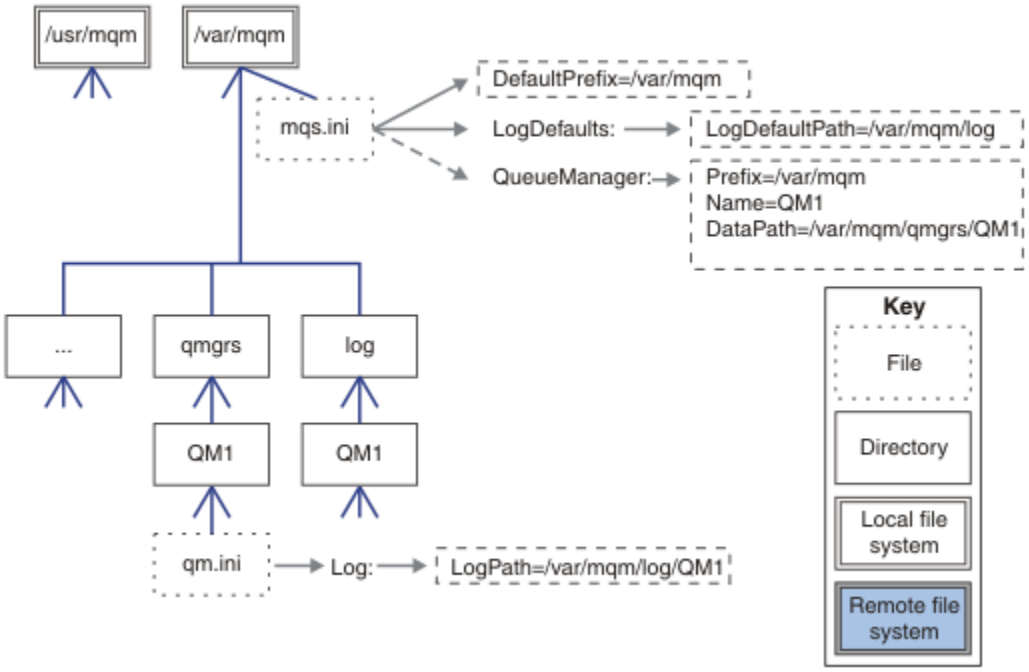
Obrázek 36. Šablona vzoru adresářové struktury

Typická adresářová struktura pro IBM MQ

Obrázek 37 na stránce 130 je výchozí adresářová struktura vytvořená v produktu IBM MQ zadáním příkazu **crtmqm** *QM1*.

Soubor `mqs.ini` má sekci pro správce front QM1 vytvořenou odkazem na hodnotu `DefaultPrefix`. Sekce `Protokol` v souboru `qm.ini` má hodnotu pro `LogPath`, nastavenou odkazem na `LogDefaultPath` v `mqs.ini`.

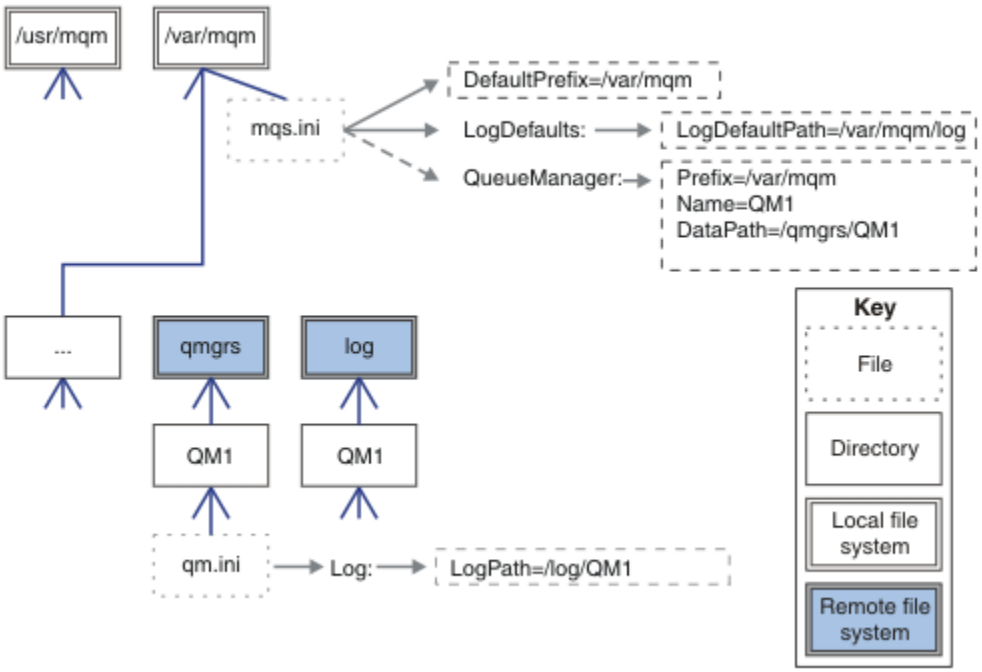
Pomocí volitelných parametrů **`crtmqm`** můžete přepsat výchozí hodnoty `DataPath` a `LogPath`.



Obrázek 37. Příklad výchozí adresářové struktury IBM MQ pro systémy AIX and Linux

Sdílet výchozí adresáře `qmgrs` a `log`

Alternativou k “Sdílet vše” na stránce 132je sdílet adresáře `qmgrs` a `log` odděleně (Obrázek 38 na stránce 131). V této konfiguraci není třeba nastavovat soubor `AMQ_MQS_INI_LOCATION` , protože výchozí soubor mqs.ini je uložen v lokálním systému souborů `/var/mqm` . Soubory a adresáře, jako např. `mqclient.ini` a `mqserver.ini` , nejsou také sdíleny.

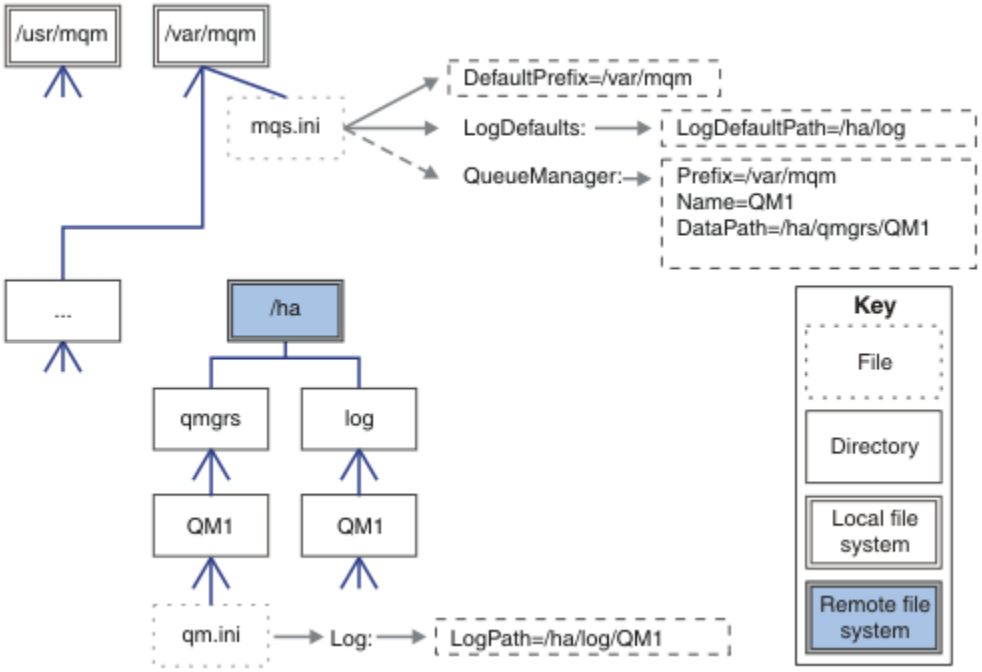


Obrázek 38. Sdílení adresářů `qmgrs` a `log`

Sdílet adresáře s názvem `qmgrs` a `log`

Konfigurace v adresáři Obrázek 39 na stránce 131 umístí `log` a `qmgrs` do společného pojmenovaného vzdáleného sdíleného systému souborů s názvem `/ha`. Stejnou fyzickou konfiguraci lze vytvořit dvěma různými způsoby.

1. Nastavte `LogDefaultPath=/ha` a pak spusťte příkaz **`crtmqm`** - `md` */ha/qmgrs* `QM1`. Výsledek je přesně tak, jak je znázorněno na obrázku Obrázek 39 na stránce 131.
2. Ponechte výchozí cesty beze změny a pak spusťte příkaz **`crtmqm`** - `ld` */ha/log* - `md` */ha/qmgrs* `QM1`.



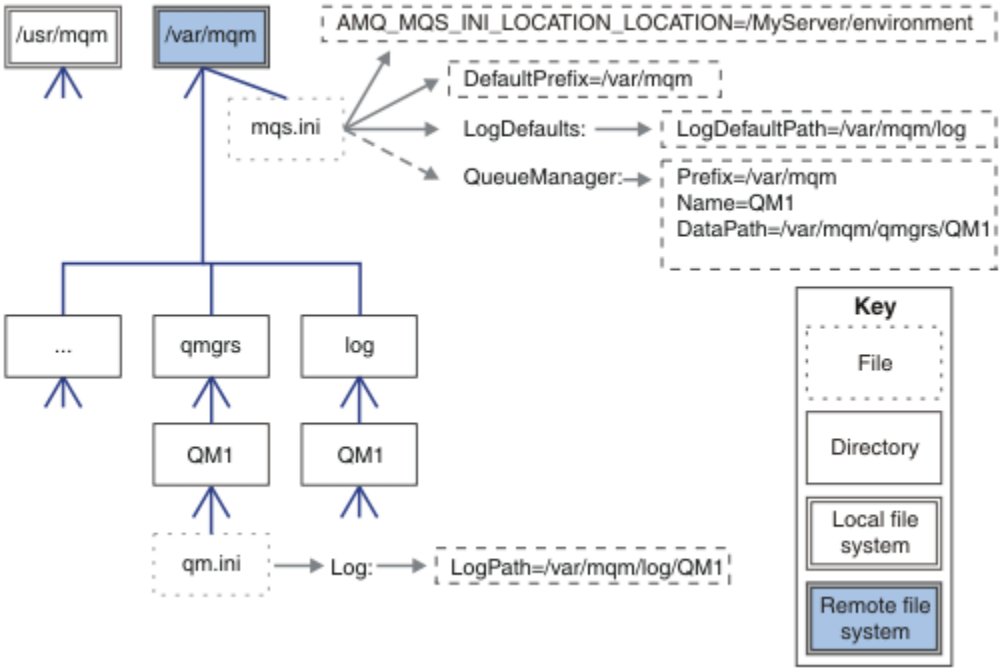
Obrázek 39. Sdílet adresáře s názvem `qmgrs` a `log`

Sdílet vše

Obrázek 40 na stránce 132 je jednoduchá konfigurace pro systém s rychlým síťovým úložištěm souborů.

Připojte `/var/mqm` jako vzdálený sdílený systém souborů. Při výchozím nastavení, když spustíte QM1, vyhledá soubor `/var/mqm`, najde jej ve sdíleném systému souborů a přečte soubor `mqs.ini` v souboru `/var/mqm`. Namísto použití jediného souboru `/var/mqm/mqs.ini` pro správce front na všech serverech můžete nastavit proměnnou prostředí `AMQ_MQS_INI_LOCATION` na jednotlivých serverech tak, aby ukazovala na různé soubory `mqs.ini` .

Poznámka: Obsah souboru generických chyb v souboru `/var/mqm/errors/` je sdílen mezi správci front na různých serverech.



Obrázek 40. Sdílet vše

Mějte na zřeteli, že toto nelze použít pro správce front s více instancemi. Důvodem je, že každý hostitel ve správci front s více instancemi musí mít vlastní lokální kopii produktu `/var/mqm` , aby mohl sledovat lokální data, jako jsou semafory a sdílená paměť. Tyto entity nelze sdílet mezi hostiteli.

Windows Adresářová struktura na systémech Windows

Jak vyhledat konfigurační informace a adresáře správce front v systému Windows.

Výchozí adresáře pro instalaci produktu IBM MQ for Windows jsou:

Adresář programu
```
C:\Program Files\IBM\MQ
```
Datový adresář
```
C:\ProgramData\IBM\MQ
```

Důležité: Windows V instalacích Windows jsou adresáře tak, jak je uvedeno, pokud zde neexistuje předchozí instalace produktu, která i nadále obsahuje položky registru nebo správce front, případně obojí. V takové situaci používá nová instalace staré umístění datových adresářů. Další informace viz Umístění programových a datových adresářů.

Chcete-li vědět, který instalační adresář a který datový adresář se používá, spusťte příkaz dspmqver .

Instalační adresář je uveden v poli **InstPath** a datový adresář je uveden v poli **DataPath** .

Po spuštění příkazu **dspmqver** se zobrazí například následující informace:

```
>dspmqver
Name:        IBM MQ
Version:     9.0.0.0
Level:       p900-L160512.4
BuildType:   IKAP - (Production)
Platform:    IBM MQ for Windows (x64 platform)
Mode:        64-bit
O/S:         Windows 7 Professional x64 Edition, Build 7601: SP1
InstName:    Installation1
InstDesc:
Primary:     Yes
InstPath:    C:\Program Files\IBM\MQ
DataPath:    C:\ProgramData\IBM\MQ
MaxCmdLevel: 900
LicenseType: Production
```

Správci front s více instancemi

Chcete-li konfigurovat správce front s více instancemi, musí být adresáře protokolů a dat umístěny v síťovém úložišti, nejlépe na jiném serveru než na libovolném serveru, na kterém jsou spuštěny instance správce front.

V příkazech **crtmqm -md** a **-ld**jsou k dispozici dva parametry, které usnadňují zadání umístění adresářů dat a protokolů správce front. Efekt zadání parametru **-md** je čtyřnásobný:

1. `mqs.ini` Sekce `QueueManager\`*`QmgrName`* obsahuje novou proměnnou *DataPath*, která ukazuje na datový adresář správce front. Na rozdíl od proměnné *Předpona* cesta zahrnuje název adresáře správce front.
2. Informace o konfiguraci správce front uložené v souboru mqs.ini jsou omezeny na *Název*, *Předpona*, *Adresář* a *DataPath*.

Windows *Obsah adresářů*

Vypisuje umístění a obsah adresářů IBM MQ .

Konfigurace IBM MQ má tři hlavní sady souborů a adresářů:

1. Spustitelný soubor a další soubory jen pro čtení, které jsou aktualizovány pouze při použití údržby. Příklad:
   - Soubor README
   - Modul plug-in a soubory nápovědy průzkumníku IBM MQ
   - Soubory s licencemi

   Tyto soubory jsou popsány v části Tabulka 16 na stránce 133.
2. Potenciálně upravitelné soubory a adresáře, které nejsou specifické pro konkrétního správce front. Tyto soubory a adresáře jsou popsány v části Tabulka 17 na stránce 134.
3. Soubory a adresáře specifické pro jednotlivé správce front na serveru. Tyto soubory a adresáře jsou popsány v části Tabulka 18 na stránce 135.

Adresáře a soubory prostředků

Adresáře a soubory prostředků obsahují veškerý spustitelný kód a prostředky pro spuštění správce front. Proměnná *FilePath*v klíči registru konfigurace IBM MQ specifickém pro instalaci obsahuje cestu k adresářům prostředků.

Tabulka 16. Adresáře a soubory v adresáři `FilePath`

Cesta k souboru	**Obsah**
FilePath\bin	Příkazy a knihovny DLL
FilePath\bin64	Příkazy a knihovny DLL (64 bitů)

Tabulka 16. Adresáře a soubory v adresáři `FilePath` (pokračování)	
Cesta k souboru	**Obsah**
FilePath\conv	Převodní tabulky dat
FilePath\doc	Soubory nápovědy průvodce
FilePath\MQExplorer	Průzkumník a Průzkumník-nápověda k modulům plug-in Eclipse
FilePath\gskit8	Sada globálního zabezpečení
FilePath\java	Prostředky Java , včetně prostředí JRE
FilePath\licenses	Informace o licenci
FilePath\Non_IBM_License	Informace o licenci
FilePath\properties	Používá se interně
FilePath\Tivoli	
FilePath\tools	Vývojové prostředky a ukázky
FilePath\web	Popsáno v části IBM MQ Console a REST API Struktura souboru komponent instalace pro neupravitelné soubory.
FilePath\Uninst	Používá se interně
FilePath\README.TXT	Soubor Readme

Adresáře nespecifické pro správce front

Některé adresáře obsahují soubory, například trasovací soubory a protokoly chyb, které nejsou specifické pro konkrétního správce front. Proměnná *DefaultPrefix* obsahuje cestu k těmto adresářům. *DefaultPrefix* je součástí sekce `AllQueueManagers` .

Tabulka 17. Adresáře a soubory v adresáři `DefaultPrefix`	
Cesta k souboru	**Obsah**
DefaultPrefix\config	Používá se interně
DefaultPrefix\conv	`ccsid_part2.tbl` a `ccsid.tbl data` řídicí soubor převodu, popsaný v části Převod dat .
DefaultPrefix\errors	Protokoly chyb mimo správce front, `AMQERR` *nn*`.LOG`
DefaultPrefix\exits	Uživatelské programy kanálu
DefaultPrefix\exits64	Programy uživatelské procedury kanálu (64 bitů)
DefaultPrefix\ipc	Nepoužitý
DefaultPrefix\qmgrs	Popsáno v tématu Tabulka 18 na stránce 135
DefaultPrefix\trace	Trasovací soubory
DefaultPrefix\web	Popsáno v části IBM MQ Console a REST API Struktura souboru komponent instalace pro uživatelem upravitelné soubory .
DefaultPrefix\amqmjpse.txt	Používá se interně

Adresáře správce front

Při vytváření správce front se vytvoří nová sada adresářů specifických pro daného správce front.

Pokud vytvoříte správce front s parametrem **-md** *filepath* , cesta se uloží do proměnné *DataPath* v sekci správce front souboru mqs.ini . Pokud vytvoříte správce front bez nastavení parametru **-md** *filepath* , adresáře správce front se vytvoří v cestě uložené v adresáři *DefaultPrefix*a cesta se zkopíruje do proměnné *Předpona* v sekci správce front souboru mqs.ini .

Tabulka 18. Adresáře a soubory v adresářích DataPath a Prefix\qmgrs\QmgrName

Cesta k souboru	**Obsah**
DataPath\@ipcc	Výchozí umístění pro tabulku připojení klienta AMQCLCHL.TAB.
DataPath\authinfo	Používá se interně.
DataPath\channel	
DataPath\clntconn	
DataPath\errors	Protokoly chyb, AMQERR *nn*.LOG
DataPath\listener	Používá se interně.
DataPath\namelist	
DataPath\plugcomp	
DataPath\procdef	
DataPath\qmanager	
DataPath\queues	
DataPath\services	
DataPath\ssl	
DataPath\startprm	
DataPath\topic	
DataPath\active	
DataPath\active.dat	
DataPath\amqalchk.fil	
DataPath\master	
DataPath\master.dat	
DataPath\qm.ini	Konfigurace správce front
DataPath\qmstatus.ini	Stav správce front
DataPath\userdata	Lze použít k uložení trvalého stavu aplikací.
Prefix\qmgrs*QmgrName*	Používá se interně
Prefix\qmgrs\@SYSTEM	Nepoužitý
Prefix\qmgrs\@SYSTEM\errors	
*DataPath**autocfg*	Používá se pro automatickou konfiguraci

IBM i Adresářová struktura na systému IBM i

Je uveden popis IFS a adresářová struktura IBM MQ IFS je popsána pro server, klienta a Java.

Integrovaný systém souborů (IFS) je součástí produktu IBM i , který podporuje proudový vstup/výstup a správu úložiště podobnou osobním počítačům, operačním systémům AIX and Linux a zároveň poskytuje integrační strukturu pro všechny informace uložené na serveru.

V systému IBM i názvy adresářů začínají znakem `& (ampersand)` místo znakem `@ (at)`. Například `@system` na IBM i je `&system`.

Kořenový systém souborů IFS pro server IBM MQ

Při instalaci produktu IBM MQ Server for IBM ise v kořenovém systému souborů IFS vytvoří následující adresáře.

ProdData:

Přehled

```
QIBM
   '-- ProdData
      '-- mqm
      '-- doc
      '-- inc
      '-- lib
      '-- samp
      '-- licenses
      '-- LicenseDoc
      '-- 5724H72_V8R0M0
```

/QIBM/ProdData/mqm
Podadresáře pod tímto obsahem obsahují všechna data produktu, například třídy C++, soubory s formátem trasování a soubory s licencemi. Data v tomto adresáři jsou odstraněna a nahrazena při každé instalaci produktu.

/QIBM/ProdData/mqm/doc
Odkaz na příkaz pro příkazy CL je uveden ve formátu HTML a nainstalován zde.

/QIBM/ProdData/mqm/inc
Hlavičkové soubory pro kompilaci programů v jazyce C nebo C + +.

/QIBM/ProdData/mqm/lib
Pomocné soubory používané produktem MQ.

/QIBM/ProdData/mqm/samp
Další vzorky.

/QIBM/ProdData/mqm/License
Soubory s licencemi. Dva soubory pro každý jazyk jsou pojmenovány jako `LA_` *xx* a `LI_` *xx* , kde *xx* je dvouznakový identifikátor jazyka pro každý dodaný jazyk.

Také následující adresář ukládá soubory licenčních smluv:

/QIBM/ProdData/LicenseDoc/5724H72_V8R0M0
Soubory s licencemi. Soubory jsou pojmenovány jako `5724H72_V8R0M0_` *xx* , kde *xx* je identifikátor jazyka o délce 2 nebo 5 znaků pro každý dodaný jazyk.

UserData:

Přehled

```
QIBM
   '-- UserData
      '-- mqm
```

```
        '-- errors
        '-- trace
        '-- qmgrs
        '-- &system
        '-- qmgrname1
        '-- qmgrname2
        '-- and so on
```

/QIBM/UserData/mqm
Podadresáře pod touto úrovní obsahují všechna uživatelská data týkající se správců front.

Při instalaci produktu se vytvoří soubor mqs.ini v adresáři /QIBM/UserData/mqm/ (pokud již neexistuje z předchozí instalace).

Při vytváření správce front se vytvoří soubor qm.ini v adresáři /QIBM/UserData/mqm/qmgrs/*QMGRNAME* /(kde *QMGRNAME* je název správce front).

Data v adresářích jsou zachována při odstranění produktu.

Kořenový systém souborů IFS pro IBM MQ MQI client

Při instalaci produktu IBM MQ MQI client for IBM ise v kořenovém systému souborů IFS vytvoří následující adresáře:

ProdData:

Přehled

```
   QIBM
      '-- ProdData
        '-- mqm
        '-- lib
```

/QIBM/ProdData/mqm
Podadresáře pod tímto adresářem obsahují všechna data produktu. Data v tomto adresáři jsou odstraněna a nahrazena pokaždé, když je produkt nahrazen.

UserData:

Přehled

```
   QIBM
      '-- UserData
        '-- mqm
        '-- errors
        '-- trace
```

/QIBM/UserData/mqm
Podadresáře pod tímto adresářem obsahují všechna uživatelská data.

Kořenový systém souborů IFS pro IBM MQ Java

Při instalaci produktu IBM MQ Java v systému IBM ijsou v kořenovém systému souborů IFS vytvořeny následující adresáře:

ProdData:

Přehled

```
   QIBM
      '-- ProdData
        '-- mqm
        '-- java
```

```
'--samples
'-- bin
'-- lib
```

/QIBM/ProdData/mqm/java
Podadresáře pod touto položkou obsahují všechna data produktu, včetně tříd Java . Data v tomto adresáři jsou odstraněna a nahrazena pokaždé, když je produkt nahrazen.

/QIBM/ProdData/mqm/java/samples
Podadresáře pod touto položkou obsahují všechny ukázkové třídy Java a data.

Knihovny vytvořené instalacemi serveru a klienta

Instalace serveru nebo klienta IBM MQ vytvoří následující knihovny:

- QMQM

  Knihovna produktů.

- QMQMSAMP

  Knihovna ukázek (pokud zvolíte instalaci ukázek).

- QMxxxx

  Pouze server.

  Při každém vytvoření správce front produkt IBM MQ automaticky vytvoří přidruženou knihovnu s názvem, například QMxxxx , kde xxxx je odvozen od názvu správce front. Tato knihovna obsahuje objekty specifické pro správce front, včetně žurnálů a přidružených zásobníků. Při výchozím nastavení je název této knihovny odvozen od názvu správce front s předponou znaků QM. Například pro správce front s názvem TEST by se knihovna měla nazývat QMTEST.

  Poznámka: Při vytváření správce front můžete zadat název jeho knihovny, pokud chcete. Příklad:

  ```
  CRTMQM MQMNAME(TEST) MQMLIB(TESTLIB)
  ```

  Příkaz WRKLIB můžete použít k vypsání všech knihoven, které IBM MQ pro IBM i vytvořil. U knihoven správce front se zobrazí text QMGR: QMGRNAME. Formát příkazu je:

  ```
  WRKLIB LIB(QM*)
  ```

  Tyto knihovny přidružené ke správci front jsou při odstranění produktu zachovány.

Multi Plánování podpory systému souborů pro produkt MFT na platformě Multiplatforms

Agenty IBM MQ Managed File Transfer MFT lze použít k přenosu dat do a ze souborů na systému souborů. Kromě toho lze monitory prostředků spuštěné v rámci agenta nakonfigurovat tak, aby monitorovaly soubory v systému souborů.

Produkt MFT vyžaduje, aby byly tyto soubory uloženy v systému souborů, který podporuje zamykání. Existují pro to dva důvody:

- Agent uzamkne soubor, aby se ujistil, že se nezmění, jakmile z něj začne číst data, nebo do něj bude zapisovat data.
- Monitory prostředků kontrolují soubory zámků, aby zkontrolovaly, zda je aktuálně nepoužívají žádné jiné procesy.

Agenti a monitory prostředků používají k provedení uzamčení Java metodu **`FileChannel.tryLock()`** a systém souborů musí být schopen uzamknout soubory, když je o to požádán pomocí tohoto volání.

Důležité: Následující systémy souborů nejsou podporovány, protože nesplňují technické požadavky produktu MFT:

- GlusterFS
- NFS verze 3

Multi Volba kruhového nebo lineárního protokolování na platformě Multiplatforms

V produktu IBM MQmůžete zvolit kruhové nebo lineární protokolování. Následující informace poskytují přehled o obou typech.

Výhody kruhového protokolování

Hlavní výhody kruhového protokolování jsou následující:

- Snadnější správa.

  Po správné konfiguraci kruhového protokolování pro vaši pracovní zátěž není nutná žádná další administrace. Zatímco v případě lineárního protokolování musí být obrazy médií zaznamenány a oblasti protokolu, které již nejsou požadovány, musí být archivovány nebo odstraněny.
- Lepší výkon

  Kruhové protokolování funguje lépe než lineární protokolování, protože kruhové protokolování je schopno znovu použít oblasti protokolu, které již byly naformátovány. Zatímco lineární protokolování musí alokovat nové oblasti protokolu a formátovat je.

Další informace viz Správa protokolů .

Výhody lineárního protokolování

Hlavní výhodou lineárního protokolování je, že lineární protokolování poskytuje ochranu před více selháními.

Kruhové ani lineární protokolování neochrání před poškozeným nebo odstraněným protokolem, ani před zprávami či frontami, které byly odstraněny aplikacemi nebo administrátorem.

Lineární protokolování (nikoli však kruhové) umožňuje zotavení poškozených objektů. Takže lineární protokolování poskytuje ochranu proti poškození nebo odstranění souborů fronty, protože tyto poškozené fronty lze obnovit z lineárního protokolu.

Jak kruhová, tak lineární ochrana proti ztrátě napájení a selhání komunikace, jak je popsáno v tématu Obnova po výpadku napájení nebo selhání komunikace.

Další aspekty

Zda zvolíte lineární nebo kruhové, závisí na tom, kolik redundance požadujete.

Výběr větší redundance, tj. lineárního protokolování, je nákladem způsobeným náklady na výkon a náklady na administraci.

Další informace viz Typy protokolování .

AIX Sdílená paměť v systému AIX

Pokud se určitým typům aplikací nepodaří připojit kvůli omezení paměti AIX , lze to ve většině případů vyřešit nastavením proměnné prostředí EXTSHM=ON.

Některé 32bitové procesy v systému AIX mohou narazit na omezení operačního systému, které ovlivňuje jejich schopnost připojit se ke správcům front systému IBM MQ . Každé standardní připojení k produktu IBM MQ používá sdílenou paměť, ale na rozdíl od jiných platforem UNIX produkt AIX umožňuje 32bitovým procesům připojit pouze 11 sad sdílené paměti.

Většina 32bitových procesů tento limit nerozpozná, ale aplikacím s vysokými požadavky na paměť se nemusí podařit připojit k produktu IBM MQ s kódem příčiny 2102: MQRC_RESOURCE_PROBLEM. Tuto chybu mohou vidět následující typy aplikací:

- Programy spuštěné ve 32bitových virtuálních počítačích Java
- Programy používající velké nebo velmi velké paměťové modely
- Programy připojující se k mnoha správcům front nebo databázím
- Programy, které se připojují k vlastním sadám sdílené paměti

Produkt 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 správců front a vašeho programu. Funkce EXTSHM=ON zabraňuje této chybě ve většině případů, ale je nekompatibilní s programy, které používají volbu SHM_SIZE funkce shmctl.

Aplikace IBM MQ MQI client a všechny 64bitové procesy nejsou tímto omezením ovlivněny. Mohou se připojit ke správcům front IBM MQ bez ohledu na to, zda byla nastavena volba EXTSHM.

Linux AIX Prostředky IBM MQ a UNIX System V IPC

Správce front používá některé prostředky IPC. Pomocí **ipcs -a** zjistíte, jaké prostředky se používají.

Tyto informace se vztahují pouze na IBM MQ spuštěné na systémech AIX and Linux .

Produkt IBM MQ používá prostředky IPC (*semafory* a *segmenty sdílené paměti*). k ukládání a předávání dat mezi systémovými komponentami. Tyto prostředky jsou používány procesy správce front a aplikacemi, které se připojují ke správci front. IBM MQ MQI clients nepoužívejte prostředky IPC, s výjimkou řízení trasování IBM MQ . Použijte UNIX příkaz **ipcs -a** , abyste získali úplné informace o počtu a velikosti prostředků IPC, které se momentálně používají na počítači.

Linux AIX IBM MQ a UNIX Priorita procesu

Doporučené postupy při nastavování hodnot priority procesu *nice* .

Tyto informace se vztahují pouze na IBM MQ spuštěné na systémech AIX and Linux .

Spustíte-li proces na pozadí, může být vyvolávajícím shellem dána vyšší hodnota *nice* (a tedy nižší priorita). To může mít obecné dopady na výkon produktu IBM MQ . V situacích s vysokou úrovní stresu platí, že pokud existuje mnoho podprocesů připravených ke spuštění s vyšší prioritou a některé s nižší prioritou, mohou charakteristiky plánování operačního systému připravit podprocesy s nižší prioritou o čas procesoru.

Je dobrým zvykem, že nezávisle spuštěné procesy přidružené ke správcům front, například **runmqlsr**, mají stejné hodnoty *nice* jako správce front, ke kterému jsou přidruženy. Ujistěte se, že shell těmto procesům na pozadí nepřiřazuje vyšší hodnotu *nice* . Například v shellu ksh použijte nastavení "`set +o bgnice`" k zastavení shellu ksh, aby zvýšil hodnotu *nice* procesů na pozadí. Hodnoty *nice* spuštěných procesů můžete ověřit kontrolou sloupce *NI* výpisu "ps -efl" .

Také spusťte procesy aplikace IBM MQ se stejnou hodnotou *nice* jako správce front. Pokud jsou spuštěny s různými hodnotami *nice* , může podproces aplikace zablokovat podproces správce front nebo naopak, což způsobí snížení výkonu.

z/OS Plánování prostředí IBM MQ na systému z/OS

Při plánování prostředí IBM MQ musíte vzít v úvahu požadavky na prostředky pro datové sady, sady stránek, Db2, zařízení Coupling Facilities a prostředky pro protokolování a zálohování. Toto téma použijte k plánování prostředí, kde je spuštěn produkt IBM MQ .

Než začnete plánovat svou architekturu IBM MQ , seznamte se se základními koncepty produktu IBM MQ for z/OS . Viz témata v části IBM MQ for z/OS koncepty.

Při plánování správce front může být nutné pracovat s různými lidmi ve vaší organizaci. Je obvykle dobré zapojit tyto lidi brzy, protože postupy kontroly změn mohou trvat dlouho. Také vám mohou sdělit, jaké parametry je třeba nakonfigurovat pro konfiguraci produktu IBM MQ for z/OS.

Například můžete potřebovat pracovat s:

- Administrátor úložiště, který určí kvalifikátor vysoké úrovně datových sad správce front a přidělí dostatek prostoru pro datové sady správce front.
- Systémový programátor z/OS definuje subsystém IBM MQ pro z/OS a autorizuje knihovny IBM MQ for z/OS .
- Administrátor sítě k určení, který zásobník TCP/IP a porty by měly být použity pro IBM MQ for z/OS.
- Administrátor zabezpečení pro nastavení přístupu k datovým sadám správce front, profilům zabezpečení pro prostředky IBM MQ for z/OS a certifikátům TLS.
- Db2 administrátor pro nastavení tabulek Db2 při konfiguraci skupiny sdílení front.

Související pojmy

IBM MQ Technický přehled

Související úlohy

“Plánování architektury IBM MQ” na stránce 5
Při plánování prostředí IBM MQ zvažte podporu, kterou produkt IBM MQ poskytuje pro jednu a více architektur správců front a pro styly systému zpráv typu point-to-point a publikování/odběr. Také naplánujte své požadavky na prostředky a použití protokolovacích a zálohovacích zařízení.

Konfigurace produktu z/OS

Správa serveruIBM MQ for z/OS

z/OS Plánování pro vašeho správce front

Při nastavování správce front by vaše plánování mělo umožnit růst správce front tak, aby splňoval potřeby vašeho podniku.

Nejlepší způsob konfigurace správce front je v následujících krocích:

1. Konfigurovat základního správce front
2. Konfigurujte inicializátor kanálu, který provádí komunikaci správce front se správcem front, a komunikaci se vzdálenou klientskou aplikací.
3. Chcete-li šifrovat a chránit zprávy, nakonfigurujte Advanced Message Security
4. Chcete-li použít přenos souborů přes produkt IBM MQ, nakonfigurujte produkt Managed File Transfer pro produkt z/OS.
5. Chcete-li použít administraci nebo systém zpráv REST APInebo IBM MQ Console ke správě IBM MQ z webového prohlížeče, nakonfigurujte server mqweb.

Některé podniky mají ve svém prostředí statisíce správců front. Síť IBM MQ musíte zvážit nyní a za pět let.

V systému z/OSNěkteří správci front zpracovávají tisíce zpráv za sekundu a protokolují více než 100 MB za sekundu. Pokud očekáváte velmi vysoké svazky, možná budete muset zvážit možnost mít více než jednoho správce front.

V systému z/OSMůže být produkt IBM MQ spuštěn jako součást skupiny sdílení front (QSG), kde jsou zprávy uloženy v prostředku Coupling Facility, a ke zprávám může přistupovat libovolný správce front ve skupině sdílení front. Chcete-li spustit ve skupině sdílení front, je třeba zvážit, kolik správců front potřebujete. Obvykle existuje jeden správce front pro každou oblast LPAR. Můžete mít také jednoho správce front, který bude pravidelně zálohovat struktury prostředku CF.

Některé změny konfigurace lze snadno provést, například definovat novou frontu. Některé jsou těžší, například zvětšování protokolů a sad stránek, a některé konfigurace nelze změnit, například název správce front nebo název skupiny sdílení front.

Informace o výkonu a vyladění jsou k dispozici v balíku MP16 performance SupportPac .

Konvence pojmenování

Musíte mít konvenci pojmenování pro datové sady správce front.

Mnoho podniků používá číslo vydání v názvu zaváděcích knihoven atd. Možná budete chtít zvážit, zda mít alias `MQM.SCSQAUTH` ukazující na aktuálně používanou verzi, jako např. `MQM.V930.SCSQAUTH`, takže při migraci na novou verzi produktu IBM MQnemusíte měnit soubory CICS, Batch a IMS JCL.

Symbolický odkaz v adresáři z/OS UNIX System Services můžete použít jako odkaz na instalační adresář pro aktuálně používanou verzi produktu IBM MQ .

Datové sady používané správcem front (protokoly, sady stránek, knihovny JCL) vyžadují konvenci pojmenování pro zjednodušení vytváření profilů zabezpečení a mapování datových sad na paměťové třídy SMS, které řídí umístění datových sad na disk, a jejich atributy.

Všimněte si, že vložení verze produktu IBM MQ do názvu sad stránek nebo protokolů není dobrý nápad. Jednou můžete provést migraci na novou verzi a datová sada bude mít "chybné" názvy.

Aplikace

Musíte pochopit obchodní aplikace a nejlepší způsob, jak nakonfigurovat produkt IBM MQ. Pokud například aplikace mají logiku pro zajištění schopnosti obnovy a opakování, pak mohou být dočasné zprávy dostatečně dobré. Chcete-li produkt IBM MQ zpracovat obnovu, musíte použít trvalé zprávy a vložit a získat zprávy v synchronizačním bodu.

Je třeba izolovat fronty od různých obchodních transakcí. Pokud se fronta pro jednu obchodní aplikaci zaplní, nechcete, aby to mělo vliv na jiné obchodní aplikace. Pokud je to možné, izolujte fronty v různých sadách stránek a fondech vyrovnávacích pamětí nebo strukturách.

Musíte pochopit profil zpráv. Pro mnoho aplikací mají fronty pouze několik zpráv. Jiné aplikace mohou během dne vytvářet fronty a mohou být zpracovány přes noc. Fronta, která má v sobě obvykle jen několik zpráv, může potřebovat mnoho hodin zpráv v hodnotě, pokud je problém a zprávy nejsou zpracovány. Chcete-li umožnit očekávanou maximální kapacitu, je třeba nastavit velikost struktur prostředku CF a sad stránek.

Po konfiguraci

Po nakonfigurování správce front (a komponent) je třeba naplánovat:

- Zálohování sad stránek.
- Zálohování definic objektů.
- Automatizace zálohování všech struktur CF.
- Monitorování zpráv IBM MQ a provedení akce, když je zjištěn problém.
- Shromažďování statistických dat IBM MQ .
- Monitorování využití prostředků, jako je virtuální úložiště, a množství protokolovaných dat za hodinu. Pomocí této volby můžete zjistit, zda se vaše využití prostředků zvyšuje a zda je třeba provést akce, například nastavení nového správce front.

z/OS Plánování požadavků na úložiště a výkon na systému z/OS

Musíte nastavit realistické a dosažitelné úložiště a výkonnostní cíle pro systém IBM MQ . Toto téma vám pomůže porozumět faktorům, které ovlivňují úložiště a výkon.

Toto téma obsahuje informace o požadavcích na úložiště a výkon pro produkt IBM MQ for z/OS. Obsahuje následující sekce:

- z/OS volby výkonu pro IBM MQ
- Určení z/OS důležitosti správy pracovní zátěže a cílů rychlosti
- “Úložiště knihovny” na stránce 143
- “Využití systémového LX” na stránce 143

- “Konfigurace úložiště” na stránce 144
- “Diskové úložiště” na stránce 149

Další informace viz “Kde najít další informace o požadavcích na úložiště a výkon” na stránce 150 .

z/OS volby výkonu pro IBM MQ

Pomocí správy pracovní zátěže můžete definovat cíle výkonu a přiřadit každému cíli obchodní důležitost. Definujete cíle pro práci v obchodních termínech a systém rozhodne, kolik prostředků, jako je procesor a úložiště, by mělo být dáno práci, aby splnila svůj cíl. Správa pracovní zátěže řídí prioritu odbavení na základě cílů, které zadáte. Správa pracovní zátěže zvýší nebo sníží prioritu podle potřeby, aby splnila určený cíl. Nemusíte tedy vyladit přesné priority každého kusu práce v systému a můžete se místo toho zaměřit na obchodní cíle.

Tři druhy cílů jsou:

Doba odezvy
Jak rychle chcete, aby byla práce zpracována

Rychlost provedení
Jak rychle by měla být práce spuštěna, když je připravena, bez zpoždění pro procesor, úložiště, přístup I/O a prodlevu fronty

diskreční
Kategorie pro práci s nízkou prioritou, pro kterou neexistují žádné výkonnostní cíle

Cíle doby odezvy jsou vhodné pro aplikace koncových uživatelů. Uživatelé produktu CICS mohou například nastavit cíle pracovní zátěže jako cíle doby odezvy. Pro adresní prostory IBM MQ jsou vhodnější cíle rychlosti. Malé množství práce provedené ve správci front se započítává do tohoto cíle rychlosti, ale tato práce je kritická pro výkon. Většina práce provedené správcem front se započítává do výkonnostního cíle aplikace koncového uživatele. Většina práce provedené adresním prostorem inicializátoru kanálu se započítává do vlastního cíle rychlosti. Příjem a odesílání zpráv IBM MQ , které iniciátor kanálu provádí, je obvykle důležité pro výkon obchodních aplikací, které je používají.

Určení cílů důležitosti a rychlosti správy pracovní zátěže produktu z/OS

Další informace viz “Určení důležitosti správy pracovní zátěže produktu z/OS” na stránce 144.

Úložiště knihovny

Musíte přidělit diskové úložiště pro knihovny produktu. Přesné údaje závisí na vaší konfiguraci a měly by zahrnovat cílové a distribuční knihovny i knihovny SMP/E.

Cílové knihovny používané produktem IBM MQ for z/OS používají formáty PDSE. Ujistěte se, že žádné cílové knihovny PDSE nejsou sdíleny mimo prostředí sysplex. Další informace o požadovaných knihovnách a jejich velikosti a požadovaném formátu naleznete v adresáři programu. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Využití systémového LX

Každý definovaný subsystém IBM MQ vyhradí při spuštění správce front jeden index LX (system linkage index) v době IPL a několik indexů linkage mimo systém. Index sestavení systému se znovu použije, když je správce front zastaven a restartován. Podobně distribuované řazení do front rezervuje jeden index nesystémového propojení. V nepravděpodobném případě, že váš systém z/OS má definována nedostatečná systémová LX, budete možná muset vzít tyto vyhrazené systémové LX v úvahu.

V případě potřeby lze počet systémových LX zvýšit nastavením parametru *NSYSLX* v systému SYS1.PARMLIB člen IEASYSxx.

z/OS *Určení důležitosti správy pracovní zátěže produktu z/OS*

Úplné informace o správě pracovní zátěže a definování cílů prostřednictvím definice služby viz.Dokumentace k produktu z/OS .

Toto téma navrhuje, jak nastavit důležitost správy pracovní zátěže z/OS a cíle rychlosti vzhledem k jiné důležité práci ve vašem systému. Další informace viz *z/OS Plánování MVS: Správa pracovní zátěže* .

Adresní prostor správce front musí být definován s vysokou prioritou, protože poskytuje služby subsystému. Inicializátor kanálu je adresním prostorem aplikace, ale obvykle má vysokou prioritu, aby se zajistilo, že zprávy odesílané vzdálenému správci front nebudou zpožděny. Advanced Message Security (AMS) také poskytuje služby subsystému a musí být definována s vysokou prioritou.

Použijte následující třídy služeb:

Výchozí třída služeb SYSSTC

- Adresní prostory VTAM a TCP/IP
- IRLM adresní prostor (IRLMPROC)

Poznámka: Adresní prostory VTAM, TCP/IP a IRLM musí mít vyšší prioritu odbavení než všechny adresní prostory DBMS, jejich připojené adresní prostory a jejich podřízené adresní prostory. Nepovolit správě pracovní zátěže snížit prioritu VTAM, TCP/IP nebo IRLM na (nebo nižší) prioritu ostatních adresních prostorů DBMS.

Cíl vysoké rychlosti a důležitost 1 pro třídu služeb s názvem, který definujete, například PRODREGN, pro následující:

- IBM MQ správce front, inicializátor kanálu a AMS adresní prostory
- Db2 (všechny adresní prostory s výjimkou adresního prostoru uložených procedur zavedených produktem Db2)
- CICS (všechny typy oblastí)
- IMS (všechny typy oblastí kromě BMP)

Cílem vysoké rychlosti je zajistit, aby startupy a restarty byly provedeny co nejrychleji pro všechny tyto adresní prostory.

Cíle rychlosti pro oblasti CICS a IMS jsou důležité pouze během spuštění nebo restartu. Po spuštění transakcí správa pracovní zátěže ignoruje cíle rychlosti CICS nebo IMS a přiřazuje priority na základě cílů doby odezvy transakcí spuštěných v regionech. Tyto transakční cíle by měly odrážet relativní prioritu implementovaných obchodních aplikací. Obvykle mohou mít hodnotu důležitosti 2. Všechny dávkové aplikace používající produkt IBM MQ by podobně měly mít cíle rychlosti a důležitost odrážející relativní prioritu obchodních aplikací, které implementují. Obvykle je význam a rychlost cíle bude menší než u PRODREGN.

z/OS *Konfigurace úložiště*

V 64bitovém adresním prostoru existuje virtuální linka s názvem "pruh" , který označuje adresu 2GB . Panel odděluje úložiště pod adresou 2GB , která se nazývá "pod pruhem", od úložiště nad adresou 2GB , která se nazývá "nad pruhem". Úložiště pod pruhem používá 31 bitovou adresovatelnost, úložiště nad pruhem používá 64 bitovou adresovatelnost.

Můžete určit limit 31bitového úložiště pomocí parametru JCL REGION a limit 64bitového úložiště pomocí parametru MEMLIMIT. Tyto zadané hodnoty lze přepsat pomocí uživatelských procedur z/OS .

Navrhovaná konfigurace úložiště

V následující tabulce jsou uvedeny doporučené hodnoty **REGION** a **MEMLIMIT** pro správce front, inicializátor kanálu a adresní prostory AMS. Tyto návrhy by měly být použity jako výchozí bod a upraveny pomocí informací v:

- “Konfigurace úložiště správce front” na stránce 145
- “Konfigurace úložiště inicializátoru kanálu na adrese IBM MQ 9.3” na stránce 147

- V 9.3.1 “Konfigurace úložiště inicializátoru kanálu z IBM MQ 9.3.1” na stránce 148

Tabulka 19. Navrhované definice pro REGION a MEMLIMIT	
adresní prostor	**Konfigurace úložiště**
Správce front	REGION=0M, MEMLIMIT=3G
Inicializátor kanálu na adrese IBM MQ 9.3.0	REGION=0M, MEMLIMIT=256M
V 9.3.1 Iniciátor kanálu z IBM MQ 9.3.1	REGION=0M, MEMLIMIT=2G
Adresní prostor AMS	REGION=0M

Správa velikosti MEMLIMIT a REGION

Další mechanizmy, například parametr **MEMLIMIT** ve členu SMFPRMxx systému SYS1.PARMLIB nebo uživatelská procedura IEFUSI mohou být použity ve vaší instalaci k poskytnutí výchozího množství virtuálního úložiště nad pruhem pro adresní prostory z/OS . Úplné podrobnosti o omezení úložiště nad pruhem viz Správa paměti nad pruhem .

z/OS *Konfigurace úložiště správce front*
Adresní prostor správce front bude pravděpodobně hlavním uživatelem 64bitového úložiště v instalaci produktu IBM MQ . Každé připojení ke správci front vyžaduje přidělení společného úložiště, jak je popsáno v následujícím textu. Kromě 64bitového úložiště byste měli povolit správci front používat veškeré dostupné 31bitové úložiště zadáním REGION=0M v JCL správce front.

Společné úložiště

Každý subsystém IBM MQ for z/OS má následující přibližné požadavky na úložiště:

- CSA 4KB
- ECSA 800KBplus velikost trasovací tabulky, která je uvedena v parametru **TRACTBL** makra systémového parametru CSQ6SYSP . Další informace viz Použití CSQ6SYSP.

Kromě toho každé souběžné logické připojení ke správci front vyžaduje přibližně 5 kB ECSA. Po ukončení úlohy mohou ostatní úlohy produktu IBM MQ znovu použít toto úložiště.

Produkt IBM MQ neuvolňuje úložiště, dokud není správce front vypnutý, takže můžete vypočítat maximální množství ECSA požadované vynásobením maximálního počtu souběžných připojení 5KB. Počet souběžných logických připojení je součtem počtu:

- Úlohy (TCB) v oblastech dávek, TSO, z/OS UNIX System Services, IMSa Db2 adresního prostoru uložených procedur (SPAS), které jsou připojeny k produktu IBM MQ, ale nejsou odpojeny.
- CICS transakcí, které vydaly požadavek IBM MQ , ale nebyly ukončeny
- JMS Připojení, relace, TopicSessions nebo QueueSessions , které byly vytvořeny (pro připojení vazeb), ale dosud nebyly zničeny nebo byly uvolněny z paměti.
- Aktivní kanály IBM MQ

Pomocí konfiguračního parametru **ACELIM** můžete nastavit omezení pro společné úložiště používané logickými připojeními ke správci front. Ovládací prvek **ACELIM** je primárně zajímavý pro servery, kde uložené procedury Db2 způsobují operace ve frontách IBM MQ .

Při řízení z uložené procedury může každá operace IBM MQ vést k novému logickému připojení ke správci front. Velké pracovní jednotky Db2 , například kvůli zatížení tabulky, mohou mít za následek nadměrnou poptávku po společném úložišti.

Produkt **ACELIM** je určen k omezení použití společné paměti a k ochraně systému z/OS omezením počtu připojení v systému. Parametr **ACELIM** byste měli nastavit pouze u správců front, u kterých bylo zjištěno, že používají nadměrné množství úložiště ECSA. Další informace viz část **ACELIM** v části *Použití CSQ6SYSP* .

Chcete-li nastavit hodnotu pro **ACELIM**, nejprve určete velikost úložiště momentálně v podfondu řízeném hodnotou **ACELIM** . Tyto informace jsou v záznamech SMF 115 podtypu 5 vytvořených pomocí trasování statistiky CLASS (3).

IBM MQ Data SMF lze formátovat pomocí SupportPac MP1B. Počet bajtů používaných v podfondu řízeném produktem **ACELIM** se zobrazí v STGPOOL DD na řádku s názvem *ACE/PEB*.

Další informace o záznamech statistiky SMF 115 viz Interpretace statistiky výkonu produktu IBM MQ for z/OS.

Zvyšte běžnou hodnotu o dostatečnou marži, abyste poskytli prostor pro růst a špičky pracovní zátěže. Vydělte novou hodnotu 1024, čímž získáte maximální velikost úložiště v kB pro použití v konfiguraci **ACELIM** .

Soukromé úložiště

Adresní prostor správce front používá 64bitové úložiště pro mnoho vnitřních řídicích bloků. Parametr **MEMLIMIT** souboru JCL správce front definuje maximální množství dostupného 64bitového úložiště. 3GB úložiště `MEMLIMIT=3G`je minimum, které byste měli použít, avšak v závislosti na vaší konfiguraci může být zapotřebí podstatně více.

Chcete-li zabránit potenciálním problémům, měli byste zadat specifickou hodnotu **MEMLIMIT** spíše než `MEMLIMIT=NOLIMIT` . Zadáte-li hodnotu `NOLIMIT` nebo velmi velkou hodnotu, bude možné využít veškeré dostupné virtuální úložiště z/OS , což povede ke stránkování v systému. Při zvyšování hodnoty parametru **MEMLIMIT** byste měli s programátorem systému z/OS projednat nové nastavení v případě, že existuje celosystémový limit množství úložiště, které lze použít.

Máte-li pro parametr **MEMLIMIT** velkou hodnotu, budete možná muset zvýšit velikost datových sad výpisu paměti, protože je ve výpisu paměti zachyceno více dat.

Využití úložiště adresního prostoru můžete monitorovat ze zprávy CSQY220I , která označuje velikost využívaného 31 a 64bitového soukromého úložiště a zbývající volné množství.

Buffer Pools, Fondy vyrovnávacích pamětí

Fondy vyrovnávacích pamětí jsou významným uživatelem soukromého úložiště v adresním prostoru správce front. Každá velikost fondu vyrovnávacích pamětí je určena v době inicializace správce front a úložiště je přiděleno pro fond vyrovnávacích pamětí, když je připojena sada stránek, která používá tento fond vyrovnávacích pamětí. Parametr **LOCATION (ABOVE|BELOW)** se používá k určení místa přidělení vyrovnávacích pamětí. Pomocí příkazu ALTER BUFFPOOL můžete dynamicky měnit velikost fondů vyrovnávacích pamětí.

Při výpočtu hodnoty parametru **MEMLIMIT** je důležité, abyste vzali v úvahu velikost fondu vyrovnávacích pamětí, pokud jsou nakonfigurovány s produktem **LOCATION(ABOVE)**. Výpočet byste měli provést následujícím způsobem.

Vypočítejte hodnotu **MEMLIMIT** jako 2GB plus velikost fondů vyrovnávacích pamětí nakonfigurovaných s produktem **LOCATION(ABOVE)**, zaokrouhlenou nahoru na nejbližší GB. Nastavte parametr MEMLIMIT na minimum 3GB a zvyšte jej podle potřeby, pokud potřebujete zvýšit velikost fondů vyrovnávacích pamětí.

Například pro tři fondy vyrovnávacích pamětí nakonfigurované s produktem **LOCATION(ABOVE)** má fond vyrovnávacích pamětí jednu 10 000 vyrovnávacích pamětí a dva a tři fondy vyrovnávacích pamětí 50 000 vyrovnávacích pamětí. Využití paměti nad pruhem se rovná 110 000 (celkový počet vyrovnávacích pamětí) * 4096 = 450 560 000 bajtů = 430MB.

Všechny fondy vyrovnávacích pamětí bez ohledu na **LOCATION** využívají 64bitové úložiště pro řídicí struktury. Vzhledem k tomu, že se počet fondů vyrovnávacích pamětí a počet vyrovnávacích pamětí v těchto fondech zvýší, může se to stát významným. Každá vyrovnávací paměť vyžaduje dalších 200 bajtů 64bitového úložiště. Pro předchozí konfiguraci, která by vyžadovala: 200 * 110 000 = 22 000 000 bajtů = 21MB.

Proto lze v tomto scénáři 3GB použít pro **MEMLIMIT**, což umožňuje rozsah růstu: 21MB + 430MB + 2GB , který zaokrouhluje až na 3GB.

Pro některé konfigurace může být použití fondů vyrovnávacích pamětí, které mají své vyrovnávací paměti trvale zálohovány reálným úložištěm, významným přínosem pro výkon. Toho lze dosáhnout zadáním hodnoty FIXED4KB pro atribut **PAGECLAS** fondu vyrovnávacích pamětí. Toto byste však měli provést pouze v případě, že je v logické oblasti k dispozici dostatek skutečného úložiště, jinak by mohlo dojít k ovlivnění jiných adresních prostorů. Chcete-li získat informace o tom, kdy byste měli použít hodnotu FIXED4KB pro **PAGECLAS**, prohlédněte si téma IBM MQ Support Pac MP16: IBM MQ for z/OS -Plánování a vyladění kapacity.

Nastavení fondů vyrovnávacích pamětí tak velkých, aby existovala stránkování MVS , může nepříznivě ovlivnit výkon. Můžete zvážit použití menšího fondu vyrovnávacích pamětí, který nestránkuje, s IBM MQ přesunutím zprávy do a ze sady stránek.

V 9.3.1 **OBNOVIT STRUKTURU CFSTRUCT**

Příkaz IBM MQ 9.3.1 **RECOVER CFSTRUCT** více využívá 64bitové úložiště. V mnoha případech by mělo být k dispozici náhradní 64bitové úložiště, a proto použití příkazu nevyžaduje zvýšení hodnoty **MEMLIMIT**. Pokud však pravděpodobně máte rozsáhlé zálohy struktury obsahující více než několik milionů zpráv, měli byste zvýšit hodnotu **MEMLIMIT** pro všechny správce front, kteří mohou zpracovat příkaz **RECOVER CFSTRUCT** o 500MB.

Pokud jste například již MEMLIMIT=3G měli, měli byste zvážit použití parametru MEMLIMIT=4G , protože parametr **MEMLIMIT** nepovoluje desetinná místa.

Vyrovnávací paměti SMDS (Shared Message Data Set) a MEMLIMIT

Při spouštění pracovní zátěže systému zpráv s použitím sdílených datových sad zpráv existují dvě úrovně optimalizace, kterých lze dosáhnout úpravou atributů DSBUFS a DSBLOCK.

Množství výše uvedeného úložiště správce front pruhu, které používá vyrovnávací paměť SMDS, je DSBUFS x DSBLOCK. To znamená, že při výchozím nastavení je pro každou strukturu CFLEVEL (5) ve správci front použito 100 x 256KB (25MB).

I když tato hodnota není příliš vysoká, pokud váš podnik nebo podniky mají mnoho CFBOS, některé z nich mohou přidělit vysokou hodnotu MEMLIMIT pro fondy vyrovnávacích pamětí a někdy mají hluboké indexované fronty, takže celkem mohou dojít k vyčerpání úložiště nad pruhem.

z/OS *Konfigurace úložiště inicializátoru kanálu na adrese IBM MQ 9.3*

Inicializátor kanálu obvykle používá mnohem méně 64bitového úložiště než správce front. Kromě 64bitového úložiště byste měli iniciátoru kanálu povolit použití veškerého dostupného 31bitového úložiště zadáním REGION=0M v JCL správce front.

Společné úložiště

Inicializátor kanálu obvykle vyžaduje použití ECSA až do velikosti 160KB.

31bitové soukromé úložiště

31bitové úložiště, které je k dispozici pro inicializátor kanálu, omezuje počet souběžných připojení, která může mít CHINIT.

Každý kanál používá přibližně 170KB rozšířené soukromé oblasti v adresním prostoru inicializátoru kanálu. Pro kanály zpráv, například odesílací nebo přijímací kanály, se úložiště zvýší o velikost zprávy, pokud jsou přeneseny zprávy větší než 32KB . Toto zvýšené úložiště se uvolní, když:

- Odesílající nebo klientský kanál vyžaduje pro 10 po sobě jdoucích zpráv méně než polovinu aktuální velikosti vyrovnávací paměti.
- Je odeslán nebo přijat prezenční signál.

Úložiště je uvolněno pro opětovné použití v rámci jazykového prostředí, avšak správce virtuálního úložiště z/OS jej nepovažuje za volné. To znamená, že horní limit počtu kanálů je závislý na velikosti zprávy a vzorcích příjmu a na omezeních jednotlivých uživatelských systémů v rozšířené soukromé oblasti.

Horní limit počtu kanálů bude na mnoha systémech pravděpodobně přibližně 9000, protože velikost rozšířené oblasti pravděpodobně nepřekročí 1.6GB. Použití velikostí zpráv větších než 32KB snižuje maximální počet kanálů v systému. Pokud jsou například přeneseny zprávy dlouhé 100MB a předpokládá se rozšířená velikost oblasti 1.6GB , maximální počet kanálů je 15.

Trasování inicializátoru kanálu je zapsáno do datového prostoru. Velikost úložiště datového prostoru je řízena parametrem **TRAXTBL** . Viz ALTER QMGR.

64bitové soukromé úložiště

Parametr MEMLIMIT inicializátoru kanálu JCL definuje maximální množství dostupného 64bitového úložiště. 256MB úložiště, MEMLIMIT=256M, je minimální hodnota, kterou byste měli použít. V závislosti na vaší konfiguraci může být zapotřebí podstatně více.

Měli byste uvést rozumnou hodnotu MEMLIMIT, spíše než MEMLIMIT = NOLIMIT, abyste předešli potenciálním problémům. Zadáte-li hodnotu NOLIMIT nebo velmi velkou hodnotu, bude možné využít veškeré dostupné virtuální úložiště z/OS , což povede ke stránkování v systému. Při zvyšování hodnoty parametru MEMLIMIT byste měli o novém nastavení diskutovat s programátorem systému z/OS v případě, že existuje celosystémový limit množství paměti, které lze použít.

Máte-li pro parametr MEMLIMIT velkou hodnotu, může být nutné zvýšit velikost datových sad výpisu paměti, protože je ve výpisu paměti zachyceno více dat.

V inicializátoru kanálu je jediný uživatel 64bitového úložiště: SMF.

SMF

Je-li tato volba povolena, evidence SMF třídy 4 nebo statistika vyžadují 64bitové úložiště. Je vyžadováno minimálně 256MB úložiště. Pokud není k dispozici dostatek paměti, iniciátor kanálu vydá zprávu CSQX124E a evidence a statistiky třídy 4 nejsou k dispozici.

Konfigurace úložiště inicializátoru kanálu z IBM MQ 9.3.1

Inicializátor kanálu obvykle používá mnohem méně 64bitového úložiště než správce front. Avšak z IBM MQ 9.3.1 se využití zvýšilo. Kromě 64bitového úložiště byste měli iniciátoru kanálu povolit použití veškerého dostupného 31bitového úložiště zadáním REGION=0M v JCL správce front.

Společné úložiště

Inicializátor kanálu obvykle vyžaduje použití ECSA až do velikosti 160KB.

31bitové soukromé úložiště

31bitové úložiště, které je k dispozici pro inicializátor kanálu, omezuje počet souběžných připojení, která může mít CHINIT.

Každý kanál používá přibližně 170KB rozšířené soukromé oblasti v adresním prostoru inicializátoru kanálu. Pro kanály zpráv, například odesílací nebo přijímací kanály, se paměť zvětšuje o velikost zprávy, pokud jsou přeneseny zprávy větší než 32KB . Toto zvýšené úložiště se uvolní, když:

- Odesílající nebo klientský kanál vyžaduje pro 10 po sobě jdoucích zpráv méně než polovinu aktuální velikosti vyrovnávací paměti.
- Je odeslán nebo přijat prezenční signál.

Úložiště je uvolněno pro opětovné použití v rámci jazykového prostředí, avšak správce virtuálního úložiště z/OS jej nepovažuje za volné. To znamená, že horní limit počtu kanálů je závislý na velikosti zprávy a vzorcích příjmu a na omezeních jednotlivých uživatelských systémů v rozšířené soukromé oblasti.

Horní limit počtu kanálů bude na mnoha systémech pravděpodobně přibližně 9000, protože velikost rozšířené oblasti pravděpodobně nepřekročí 1.6GB.

Trasování inicializátoru kanálu je zapsáno do datového prostoru. Velikost úložiště datového prostoru je řízena parametrem **TRAXTBL** . Viz ALTER QMGR.

64bitové soukromé úložiště

Parametr MEMLIMIT inicializátoru kanálu JCL definuje maximální množství dostupného 64bitového úložiště. 2 GB úložiště, MEMLIMIT=2 GB, je minimální hodnota, kterou byste měli použít. V závislosti na vaší konfiguraci může být zapotřebí podstatně více.

Měli byste uvést rozumnou hodnotu MEMLIMIT, spíše než MEMLIMIT = NOLIMIT, abyste předešli potenciálním problémům. Zadáte-li hodnotu NOLIMIT nebo velmi velkou hodnotu, bude možné využít veškeré dostupné virtuální úložiště z/OS , což povede ke stránkování v systému. Při zvyšování hodnoty parametru MEMLIMIT byste měli o novém nastavení diskutovat s programátorem systému z/OS v případě, že existuje celosystémový limit množství paměti, které lze použít.

Máte-li pro parametr MEMLIMIT velkou hodnotu, může být nutné zvýšit velikost datových sad výpisu paměti, protože je ve výpisu paměti zachyceno více dat.

V inicializátoru kanálu jsou dva uživatelé 64bitového úložiště: kanály SMF a kanály připojení serveru.

SMF

Je-li tato volba povolena, evidence SMF třídy 4 nebo statistika vyžadují 64bitové úložiště. Je vyžadováno minimálně 256MB úložiště. Pokud není k dispozici dostatek paměti, iniciátor kanálu vydá zprávu CSQX124E a evidence a statistiky třídy 4 nejsou k dispozici.

Kanály připojení serveru

Kanály připojení serveru IBM MQ 9.3.1 přidělují vyrovnávací paměti zpráv v 64bitovém úložišti, pokud přenášejí zprávy o velikosti větší než 32 kB.

Tyto vyrovnávací paměti jsou uvolněny, pokud kanály vyžadují méně než polovinu aktuální velikosti vyrovnávací paměti pro 10 po sobě jdoucích zpráv nebo pokud je odeslán nebo přijat prezenční signál.

Hodnota MEMLIMIT nastavuje horní limit počtu souběžných kanálů připojení serveru. Měli byste použít minimální hodnotu MEMLIMIT=2G , abyste se ujistili, že může být spuštěn stejný počet kanálů jako v předchozích verzích produktu IBM MQ 9.3.1, a také abyste poskytli určitou kapacitu pro růst.

Přibližnou hodnotu parametru MEMLIMIT můžete vypočítat tak, že vypracujete maximální maximální počet souběžně aktivních kanálů připojení serveru a pro tyto kanály maximální velikost zprávy, kterou od nich očekáváte, že budou přenášet. Jako počáteční bod a zaokrouhlení byste měli použít MEMLIMIT=2GB .

Pokud například nastavíte maximální počet souběžných kanálů připojení serveru na 2 000 a každý kanál bude mít maximální velikost zprávy 1MB, budou kanály připojení serveru používat maximum těsně pod 2GB 64bitového úložiště. Vzhledem k tomu, že se tato hodnota velmi blíží hodnotě 2GB , měli byste zaokrouhlit až na hodnotu MEMLIMIT=3G.

z/OS *Diskové úložiště*

Toto téma použijte při plánování požadavků na diskové úložiště pro datové sady protokolů, úložiště Db2 , úložiště prostředku Coupling Facility a datové sady stránek.

Ve spolupráci s administrátorem úložiště určete umístění datových sad správce front. Administrátor úložiště vám může například poskytnout specifické svazky DASD nebo třídy úložiště SMS, třídy dat a třídy správy pro různé typy datových sad.

- Datové sady protokolu musí být na DASD. Tyto protokoly mohou mít vysokou aktivitu I/O s malou dobou odezvy a nemusí být zálohovány.

- Archivní protokoly mohou být na DASD nebo pásce. Poté, co byly vytvořeny, nemusí být nikdy znovu čteny, s výjimkou nestandardních situací, jako je například obnova sady stránek ze zálohy. Měly by mít dlouhé datum uchování.
- Sady stránek mohou mít nízkou až střední aktivitu a měly by být pravidelně zálohovány. Na vysoce používaném systému by měly být zálohovány dvakrát denně.
- Datové sady BSDS by měly být zálohovány denně; nemají vysokou aktivitu I/O.

Všechny datové sady jsou podobné těm, které používá produkt Db2, a podobné procedury údržby lze použít pro produkt IBM MQ.

Podrobnosti o plánování datového úložiště naleznete v následujících sekcích:

- **Protokoly a archivní úložiště**

  Téma “Jak dlouho musím uchovávat archivní protokoly” na stránce 167 popisuje, jak určit, kolik úložného prostoru vyžadují datové sady aktivního protokolu a archivu, v závislosti na objemu zpráv, které systém IBM MQ zpracovává, a jak často jsou aktivní protokoly ukládány do datových sad archivu.
- **Db2 úložiště**

  “Db2 úložný prostor” na stránce 184 popisuje, jak určit, kolik úložiště Db2 vyžaduje pro data IBM MQ .
- **úložiště prostředku Coupling Facility**

  “Definování prostředků prostředku Coupling Facility” na stránce 174 popisuje, jak lze určit, jak velké struktury prostředku Coupling Facility vytvořit.
- **Sada stránek a úložiště zpráv**

  “Plánování sad stránek a fondů vyrovnávacích pamětí” na stránce 150 popisuje, jak určit, kolik paměti datové sady stránek vyžadují, v závislosti na velikosti zpráv, které si vaše aplikace vyměňují, na počtu těchto zpráv a na rychlosti, s jakou jsou vytvářeny nebo vyměňovány.

z/OS *Kde najít další informace o požadavcích na úložiště a výkon*

Toto téma použijte jako odkaz k vyhledání dalších informací o požadavcích na úložiště a výkon.

Další informace naleznete z následujících zdrojů:

Tabulka 20. Kde najít další informace o požadavcích na úložiště

Téma	**Kam se podívat**
Parametry systému	Použití CSQ6SYSP a přizpůsobení správců front
Úložiště potřebné k instalaci produktu IBM MQ	Adresář programu. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.
Východy IEALIMIT a IEFUSI	Viz IEALIMIT a IEFUSI v dokumentaci *z/OS:MVS Instalační procedury* .
Nejnovější informace	IBM MQ SupportPac SupportPac SupportPacs pro IBM MQ a další oblasti projektu.
Správa pracovní zátěže a definování cílů prostřednictvím definice služby	*z/OS Plánování MVS: Správa pracovní zátěže*

z/OS Plánování sad stránek a fondů vyrovnávacích pamětí

Informace, které vám pomohou s plánováním počátečního počtu a velikostí datových sad stránek a fondů vyrovnávacích pamětí.

Toto téma obsahuje následující sekce:

- “Plánování sad stránek” na stránce 151

  - Použití sady stránek
  - Počet sad stránek
  - Velikost sad stránek
  - Plánování z/OS šifrování datové sady
- “Vypočítejte velikost sad stránek” na stránce 152
  - Sada stránek nula
  - Sada stránek 01-99
  - Výpočet požadavků na úložiště pro zprávy
- “Povolení expanze dynamické sady stránek” na stránce 154
- “Definování fondů vyrovnávacích pamětí” na stránce 155

Plánování sad stránek

Použití sady stránek

V případě zpráv s krátkou životností se v sadě stránek obvykle používá několik stránek a pro datové sady existuje jen malý nebo žádný vstup/výstup s výjimkou při spuštění, během kontrolního bodu nebo při ukončení práce systému.

V případě zpráv s dlouhou životností jsou stránky obsahující zprávy obvykle zapisovány na disk. Tuto operaci provádí správce front za účelem zkrácení doby restartování.

Krátkodobé zprávy oddělte od zpráv s dlouhou životností jejich umístěním do různých sad stránek a do různých fondů vyrovnávacích pamětí.

Počet sad stránek

Použití několika velkých sad stránek může usnadnit roli administrátora produktu IBM MQ , protože to znamená, že potřebujete méně sad stránek, což zjednodušuje mapování front na sady stránek.

Použití více menších sad stránek má řadu výhod. Zálohování například trvá kratší dobu a operace I/O lze provádět paralelně během zálohování a restartování. Mějte však na paměti, že se tím zvyšují významné náklady na výkon role administrátora produktu IBM MQ , který je povinen mapovat každou frontu na jeden z mnohem většího počtu sad stránek.

Definujte alespoň pět sad stránek takto:

- Sada stránek vyhrazená pro definice objektů (sada stránek nula)
- Sada stránek pro zprávy související se systémem
- Sada stránek pro zprávy s dlouhou životností kritické pro výkon
- Sada stránek pro zprávy s krátkou životností kritické pro výkon
- Sada stránek pro všechny ostatní zprávy

“Definování fondů vyrovnávacích pamětí” na stránce 155 vysvětluje výkonnostní výhody distribuce zpráv na sady stránek tímto způsobem.

Velikost sad stránek

Definujte dostatečný prostor v sadách stránek pro očekávanou maximální kapacitu zpráv. Zvažte případnou neočekávanou špičkovou kapacitu, například při vytváření zpráv, protože program serveru front není spuštěn. To lze provést přidělením sady stránek se sekundárními oblastmi nebo povolením rozšíření dynamické sady stránek. Další informace viz téma “Povolení expanze dynamické sady stránek” na stránce 154. Je obtížné zmenšit sadu stránek, takže je často lepší přidělit menší sadu stránek a umožnit její rozšíření v případě potřeby.

Při plánování velikostí sad stránek zvažte všechny zprávy, které mohou být generovány, včetně dat zpráv mimo aplikaci. Můžete například spouštět zprávy, zprávy událostí a všechny zprávy sestav, které vaše aplikace požadovala.

Velikost sady stránek určuje dobu potřebnou k obnovení sady stránek při obnově ze zálohy, protože obnova velké sady stránek trvá déle.

Poznámka: Zotavení sady stránek závisí také na době, kterou správce front potřebuje ke zpracování záznamů protokolu zapsaných od doby, kdy byla provedena záloha. Toto časové období je určeno frekvencí zálohování. Další informace viz téma “Plánování zálohování a obnovy” na stránce 186.

Poznámka: Sady stránek větší než 4 GB vyžadují použití rozšířené adresovatelnosti SMS.

Plánování šifrování datové sady z/OS

Funkci šifrování datové sady z/OS můžete použít na sady stránek pro správce front spuštěné v produktu IBM MQ for z/OS 9.1.4 nebo novějším.

Tyto sady stránek musíte přidělit pomocí atributů EXTENDED a popisku klíče datové sady, který zajistí, že data budou šifrována pomocí AES.

Viz část důvěrnost pro data v klidu na systému IBM MQ for z/OS se šifrováním datové sady. Další informace viz.

Vypočítejte velikost sad stránek

Pro definice objektů správce front (například fronty a procesy) je snadné vypočítat požadavek na úložiště, protože tyto objekty mají pevnou velikost a jsou trvalé. U zpráv je však výpočet složitější z následujících důvodů:

- Velikost zpráv se liší.
- Zprávy jsou přechodné.
- Prostor obsazený zprávami, které byly načteny, je pravidelně uvolňován asynchronním procesem.

Velké sady stránek větší než 4 GB, které poskytují dodatečnou kapacitu pro zprávy, pokud se síť zastaví, lze v případě potřeby vytvořit. Existující sady stránek nelze upravit. Místo toho musí být vytvořeny nové sady stránek s rozšířenou adresovatelností a atributy rozšířeného formátu. Nové sady stránek musí mít stejnou fyzickou velikost jako staré a staré sady stránek musí být zkopírovány do nových. Je-li požadována zpětná migrace, nesmí být změněna sada stránek nula. Pokud jsou sady stránek menší než 4 GB, není potřeba žádná akce.

Sada stránek nula

Sada stránek nula je vyhrazena pro definice objektů.

Pro nulovou sadu stránek je požadované úložiště:

```
   (maximum number of local queue definitions x 1010)
      (excluding shared queues)
+  (maximum number of model queue definitions x 746)
+  (maximum number of alias queue definitions x 338)
+  (maximum number of remote queue definitions x 434)
+  (maximum number of permanent dynamic queue definitions x 1010)
+  (maximum number of process definitions x 674)
+  (maximum number of namelist definitions x 12320)
+  (maximum number of message channel definitions x 2026)
+  (maximum number of client-connection channel definitions x 5170)
+  (maximum number of server-connection channel definitions x 2026)
+  (maximum number of storage class definitions x 266)
+  (maximum number of authentication information definitions x 1010)
+  (maximum number of administrative topic definitions x 15000)
+  (total length of topic strings defined in administrative topic definitions)
```

Chcete-li určit počet záznamů, které mají být určeny v klastru pro datovou sadu sady stránek, vydělte tuto hodnotu číslem 4096.

Nemusíte povolovat objekty, které jsou uloženy ve sdíleném úložišti, ale musíte povolit objekty, které jsou uloženy nebo zkopírovány do sady stránek nula (objekty s dispozicí GROUP nebo QMGR).

Celkový počet objektů, které můžete vytvořit, je omezen kapacitou sady stránek nula. Počet lokálních front, které můžete definovat, je omezen na 524 287.

Sady stránek 01-99

Pro sady stránek 01-99 je úložiště požadované pro každou sadu stránek určeno počtem a velikostí zpráv uložených v této sadě stránek. (Zprávy ve sdílených frontách nejsou uloženy v sadách stránek.)

Chcete-li určit počet záznamů, které mají být určeny v klastru pro datovou sadu sady stránek, vydělte tuto hodnotu číslem 4096.

Výpočet požadavků na úložiště pro zprávy

Tento oddíl popisuje, jak jsou zprávy ukládány na stránky. Základní informace vám mohou pomoci vypočítat, kolik úložiště sady stránek musíte pro zprávy definovat. Chcete-li vypočítat přibližný prostor vyžadovaný pro všechny zprávy v sadě stránek, musíte zvážit maximální délku fronty všech front, které jsou mapovány na sadu stránek, a průměrnou velikost zpráv v těchto frontách.

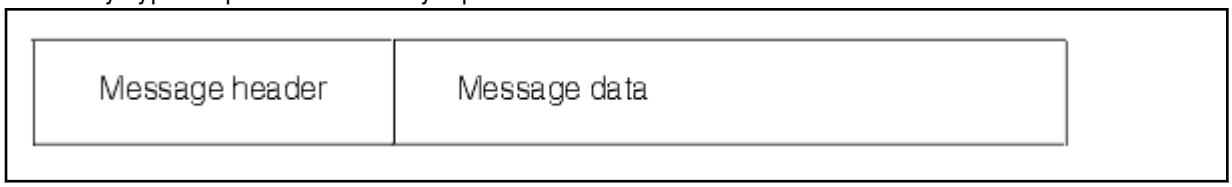
Poznámka: Velikost struktur a kontrolní informace uvedené v tomto oddíle se mohou mezi hlavními verzemi měnit. Podrobnosti specifické pro vaši verzi produktu IBM MQviz SupportPac MP16 - IBM MQ pro z/OS Plánování kapacity & ladění a IBM MQ Sestavy výkonu .

Musíte povolit možnost, že zpráva "gets" může být zpožděna z důvodů mimo kontrolu IBM MQ (například kvůli problému s vaším komunikačním protokolem). V tomto případě může míra "vložení" zpráv daleko překročit míru "získání". To může vést k velkému nárůstu počtu zpráv uložených v sadách stránek a následnému nárůstu požadované velikosti úložiště.

Každá stránka v sadě stránek má délku 4096 bajtů. Při povolení pevných informací o hlavičkách má každá stránka k dispozici 4057 bajtů prostoru pro ukládání zpráv.

Při výpočtu prostoru potřebného pro každou zprávu je třeba nejprve zvážit, zda se zpráva vejde na jednu stránku (krátká zpráva) nebo zda je třeba ji rozdělit na dvě nebo více stránek (dlouhá zpráva). Když jsou zprávy rozděleny tímto způsobem, musíte povolit další řídicí informace ve výpočtech prostoru.

Pro účely výpočtu prostoru může být zpráva znázorněna takto:



Sekce záhlaví zprávy obsahuje deskriptor zprávy a další řídicí informace, jejichž velikost se liší v závislosti na velikosti zprávy. Sekce dat zprávy obsahuje všechna skutečná data zprávy a všechna další záhlaví (například záhlaví přenosu nebo záhlaví mostu IMS).

Pro řídicí informace sady stránek jsou vyžadovány minimálně dvě stránky, což je obvykle méně než 1% celkového prostoru potřebného pro zprávy.

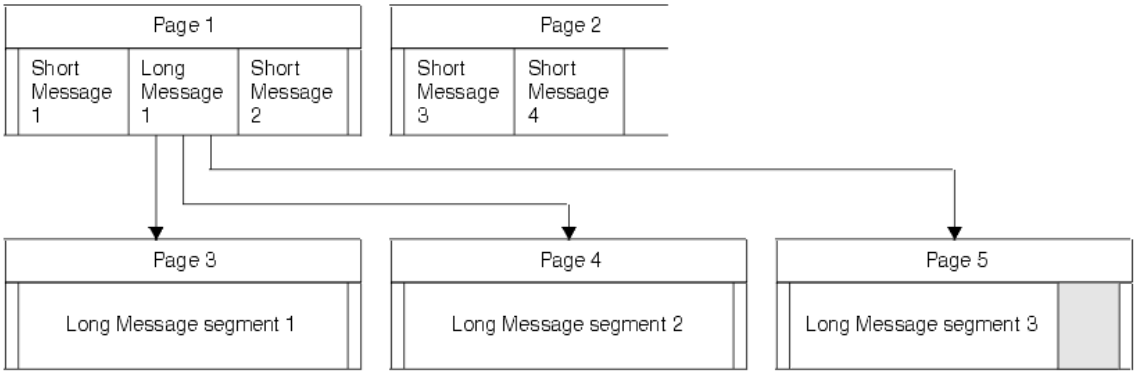
Krátké zprávy

Krátká zpráva je definována jako zpráva, která se vejde na jednu stránku.

Malé zprávy jsou uloženy na každé stránce.

Dlouhé zprávy

Pokud je velikost dat zprávy větší než 3596 bajtů, ale ne větší než 4 MB, je zpráva klasifikována jako dlouhá zpráva. Je-li zpráva prezentována s dlouhou zprávou, produkt IBM MQ uloží zprávu na řadu stránek a uloží řídicí informace, které na tyto stránky ukazují stejným způsobem, jakým by uložila krátkou zprávu. Toto je zobrazeno v části Obrázek 41 na stránce 154:



Obrázek 41. Jak produkt IBM MQ ukládá dlouhé zprávy na sady stránek

Velmi dlouhé zprávy

Velmi dlouhé zprávy jsou zprávy s velikostí větší než 4 MB. Ty jsou uloženy tak, aby každé 4 MB používala 1037 stránek. Jakýkoli zbytek je uložen stejným způsobem jako dlouhá zpráva, jak je popsáno výše.

z/OS *Povolení expanze dynamické sady stránek*

Sady stránek lze dynamicky rozšiřovat za běhu správce front. Sada stránek může mít 123 oblastí pro rozšíření a může být rozložena na více diskových svazcích.

Pokaždé, když se sada stránek rozbalí, použije se nová oblast datové sady. Správce front pokračuje v rozšiřování sady stránek v případě potřeby, dokud není dosaženo maximálního počtu oblastí pro rozšíření nebo dokud není k dispozici žádné další úložiště pro přidělení na vhodných svazcích.

Jakmile dojde k selhání rozšíření sady stránek z jednoho z výše uvedených důvodů, označí správce front sadu stránek bez dalších pokusů o rozšíření. Toto označení lze resetovat změnou nastavení stránky na EXPAND (SYSTEM).

Rozšíření sady stránek probíhá asynchronně pro všechny ostatní aktivity sady stránek, když je přiděleno 90% existujícího prostoru v sadě stránek.

Proces rozšíření sady stránek formátuje nově přidělenou oblast pro rozšíření a zpřístupní ji pro použití správcem front. Žádný z prostorů však není k dispozici pro použití, dokud nebude zformátován celý rozsah. To znamená, že rozšíření z velké části bude pravděpodobně nějakou dobu trvat, a vložení aplikací může "blokovat", pokud vyplní zbývajících 10% sady stránek před dokončením rozšíření.

Ukázka thlqual.SCSQPROC(CSQ4PAGE) ukazuje, jak definovat sekundární oblasti pro rozšíření.

Chcete-li řídit velikost nových oblastí, použijte jednu z následujících voleb klíčového slova EXPAND příkazu DEFINE PSID a ALTER PSID:

- UŽIVATEL
- SYSTÉM
- ŽÁDNÉ

UŽIVATEL

Používá velikost sekundární oblasti určenou při přidělení sady stránek. Pokud nebyla zadána hodnota nebo byla zadána hodnota nula, nemůže dojít k expanzi dynamické sady stránek.

K rozbalení sady stránek dochází, když je prostor na stránce 90% využitý a provádí se asynchronně s ostatními aktivitami sady stránek.

To může vést k rozšíření o více než jednu oblast najednou.

Zvažte následující příklad: přidělíte sadu stránek s primárním rozsahem 100 000 stránek a sekundárním rozsahem 5000 stránek. Je vložena zpráva, která vyžaduje 9999 stránek. Pokud sada

stránek již používá 85 000 stránek, bude při zápisu zprávy překročena hranice 90% (90 000 stránek). V tomto bodě je další sekundární oblast přidělena primárnímu rozsahu 100 000 stránek, přičemž velikost sady stránek je 105 000 stránek. Zbývajících 4999 stránek zprávy bude i nadále zapsáno. Když využitý stránkovací prostor dosáhne 94 500 stránek, což je 90% aktualizované velikosti sady stránek 105 000 stránek, alokuje se dalších 5 000 oblastí stránek, přičemž velikost sady stránek bude 110 000 stránek. Na konci operace MQPUT byla sada stránek dvakrát rozšířena a bylo použito 94 500 stránek. Nebyly použity žádné stránky v rozšíření druhé sady stránek, i když byly přiděleny.

Pokud bude v okamžiku opětného spuštění dříve používaná sada stránek nahrazena menší datovou sadou, bude rozšiřována, dokud nedosáhne velikosti sady dat používané dříve. K dosažení této velikosti je potřebná pouze jedna oblast.

SYSTÉM

Ignoruje velikost sekundární oblasti, která byla určena při definování sady stránek. Místo toho správce front nastaví hodnotu, která je přibližně 10% aktuální velikosti sady stránek. Hodnota je zaokrouhlena nahoru na nejbližší válec DASD.

Pokud nebyla zadána žádná hodnota nebo byla zadána hodnota nula, může stále dojít k dynamickému rozšíření sady stránek. Správce front nastaví hodnotu, která je přibližně 10% aktuální velikosti sady stránek. Nová hodnota je zaokrouhlena nahoru v závislosti na charakteristice DASD.

K expanzi sady stránek dochází, když je prostor v sadě stránek přibližně 90% využitý a provádí se asynchronně s ostatními aktivitami sady stránek.

Pokud bude v okamžiku opětného spuštění dříve používaná sada stránek nahrazena menší datovou sadou, bude rozšiřována, dokud nedosáhne velikosti sady dat používané dříve.

ŽÁDNÉ

Žádné další rozšíření sady stránek se neprovádí.

Související odkazy

ALTER PSID
PŘEDEFINOVÁNO PSID
DISPLAYUSAGE-použití

Definování fondů vyrovnávacích pamětí

Toto téma vám pomůže naplánovat počet fondů vyrovnávacích pamětí, které byste měli definovat, a jejich nastavení.

Toto téma je rozděleno do následujících sekcí:

1. “Rozhodnout o počtu fondů vyrovnávacích pamětí, které mají být definovány” na stránce 155
2. “Rozhodnout o nastavení pro každý fond vyrovnávacích pamětí” na stránce 156
3. “Monitorovat výkon fondů vyrovnávacích pamětí při očekávaném zatížení” na stránce 157
4. “Upravit charakteristiky fondu vyrovnávacích pamětí” na stránce 157

Rozhodnout o počtu fondů vyrovnávacích pamětí, které mají být definovány

Nejprve byste měli definovat čtyři fondy vyrovnávacích pamětí:

Fond vyrovnávacích pamětí 0

Používá se pro definice objektů (v sadě stránek nula) a pro fronty zpráv související se systémem, které jsou kritické z hlediska výkonu, jako např. SYSTEM.CHANNEL.SYNCQ a SYSTEM.CLUSTER.COMMAND.QUEUE a SYSTEM.CLUSTER.REPOSITORY.QUEUE .

Je však důležité vzít v úvahu bod “7” na stránce 158 v části *Upravit charakteristiku fondu vyrovnávacích pamětí* , pokud se má použít velký počet kanálů nebo klastrování.

Pro uživatelské zprávy použijte zbývající tři fondy vyrovnávacích pamětí.

Fond vyrovnávacích pamětí 1

Používá se pro důležité zprávy s dlouhou životností.

Zprávy s dlouhou životností jsou ty zprávy, které zůstávají v systému déle než dva kontrolní body, přičemž jsou zapsány do sady stránek. Máte-li mnoho zpráv s dlouhou životností, měl by být tento fond vyrovnávacích pamětí relativně malý, aby byl vstup/výstup sady stránek rovnoměrně distribuován (starší zprávy jsou zapisovány na server DASD při každém zaplnění fondu vyrovnávacích pamětí z 85%).

Je-li fond vyrovnávacích pamětí příliš velký a fond vyrovnávacích pamětí se nikdy nezaplní na 85%, je vstup/výstup sady stránek zpožděn až do zpracování kontrolního bodu. To může ovlivnit dobu odezvy v celém systému.

Pokud očekáváte pouze několik zpráv s dlouhou životností, definujte tento fond vyrovnávacích pamětí tak, aby byl dostatečně velký pro uchování všech těchto zpráv.

Fond vyrovnávacích pamětí 2
Používá se pro zprávy s krátkou životností, které jsou kritické pro výkon.

Obvykle se používá vysoký stupeň opětovného použití vyrovnávací paměti s použitím několika vyrovnávacích pamětí. Měli byste však tento fond vyrovnávacích pamětí nastavit jako velký, aby umožňoval neočekávanou akumulaci zpráv, například pokud dojde k selhání serverové aplikace.

Fond vyrovnávacích pamětí 3
Použijte pro všechny ostatní (obvykle nekritické) zprávy o výkonu.

Fronty, jako např. fronta nedoručených zpráv, SYSTEM.COMMAND.* front a SYSTEM.ADMIN.* fronty lze také mapovat na fond vyrovnávacích pamětí 3.

Tam, kde existují omezení virtuálního úložiště a fondy vyrovnávacích pamětí musí být menší, je fond vyrovnávacích pamětí 3 prvním kandidátem na snížení velikosti.

Je možné, že budete muset definovat další fondy vyrovnávacích pamětí za následujících okolností:

- Pokud je známo, že určitá fronta vyžaduje izolaci, možná proto, že vykazuje různé chování v různých časech.
  - Taková fronta může buď vyžadovat nejlepší možný výkon za různých okolností, nebo musí být izolována tak, aby neovlivňovala ostatní fronty ve fondu vyrovnávacích pamětí.
  - Každá taková fronta může být izolována do vlastního fondu vyrovnávacích pamětí a sady stránek.
- Chcete vzájemně izolovat různé sady front z důvodů provozní třídy.
  - Každá sada front pak může vyžadovat jeden nebo oba dva typy fondů vyrovnávacích pamětí 1 nebo 2, jak je popsáno v tématu Doporučené definice pro nastavení fondu vyrovnávacích pamětí, což vyžaduje vytvoření několika fondů vyrovnávacích pamětí specifického typu.

Rozhodnout o nastavení pro každý fond vyrovnávacích pamětí

Používáte-li čtyři fondy vyrovnávacích pamětí popsané v tématu “Rozhodnout o počtu fondů vyrovnávacích pamětí, které mají být definovány” na stránce 155, Doporučené definice pro nastavení fondu vyrovnávacích pamětí zobrazí dvě sady hodnot pro velikost fondů vyrovnávacích pamětí.

První sada je vhodná pro testovací systém, druhá pro produkční systém nebo systém, který se nakonec stane výrobním systémem. Ve všech případech definujte fondy vyrovnávacích pamětí pomocí atributu **LOCATION**(*ABOVE*).

Tabulka 21. Navrhované definice pro nastavení fondu vyrovnávacích pamětí

Nastavení definice	Zkušební systém	Výrobní systém
FOND vyrovnávacích pamětí 0	1 050 vyrovnávacích pamětí	50 000 vyrovnávacích pamětí
FOND vyrovnávacích pamětí 1	1 050 vyrovnávacích pamětí	20 000 vyrovnávacích pamětí
FOND vyrovnávacích pamětí 2	1 050 vyrovnávacích pamětí	50 000 vyrovnávacích pamětí

Tabulka 21. Navrhované definice pro nastavení fondu vyrovnávacích pamětí (pokračování)		
Nastavení definice	**Zkušební systém**	**Výrobní systém**
FOND vyrovnávacích pamětí 3	1 050 vyrovnávacích pamětí	20 000 vyrovnávacích pamětí

Potřebujete-li více než čtyři navrhované fondy vyrovnávacích pamětí, vyberte fond vyrovnávacích pamětí (1 nebo 2), který nejpřesněji popisuje očekávané chování front ve fondu vyrovnávacích pamětí, a jeho velikost podle informací v části Doporučené definice pro nastavení fondu vyrovnávacích pamětí.

Ujistěte se, že je parametr MEMLIMIT nastaven dostatečně vysoko, aby se všechny fondy vyrovnávacích pamětí mohly nacházet nad pruhem.

Monitorovat výkon fondů vyrovnávacích pamětí při očekávaném zatížení

Využití fondů vyrovnávacích pamětí můžete monitorovat pomocí analýzy statistiky výkonu fondu vyrovnávacích pamětí. Zejména byste měli zajistit, aby fondy vyrovnávacích pamětí byly dostatečně velké, aby hodnoty QPSTSOS, QPSTSTLA a QPSTDMC zůstaly na nule.

Další informace viz Datové záznamy správce vyrovnávací paměti.

Upravit charakteristiky fondu vyrovnávacích pamětí

V případě potřeby upravte nastavení fondu vyrovnávacích pamětí v souboru “Rozhodnout o nastavení pro každý fond vyrovnávacích pamětí” na stránce 156pomocí následujících bodů.

Jako vodítko použijte statistiku výkonu z produktu “Monitorovat výkon fondů vyrovnávacích pamětí při očekávaném zatížení” na stránce 157 .

1. Provádíte-li migraci z dřívější verze produktu IBM MQ, změňte existující nastavení pouze v případě, že máte k dispozici více skutečného úložiště.
2. Obecně platí, že větší fondy vyrovnávacích pamětí jsou lepší z hlediska výkonu a fondy vyrovnávacích pamětí mohou být mnohem větší, pokud jsou nad pruhem.

   Vždy byste však měli mít k dispozici dostatek skutečného úložiště, aby fondy vyrovnávacích pamětí byly rezidentní v reálném úložišti. Je lepší mít menší fondy vyrovnávacích pamětí, které nevedou ke stránkování, než ty velké.

   Navíc neexistuje žádný bod, který by měl fond vyrovnávacích pamětí, který by byl větší než celková velikost sad stránek, které jej používají, i když byste měli vzít v úvahu rozšíření sady stránek, pokud k němu pravděpodobně dojde.
3. Cíl pro jednu sadu stránek pro každý fond vyrovnávacích pamětí, protože poskytuje lepší izolaci aplikace.
4. Máte-li dostatek skutečného úložiště tak, aby vaše fondy vyrovnávacích pamětí nebyly operačním systémem nikdy odloženy do paměti, zvažte použití vyrovnávacích pamětí s pevnou stránkou ve vašem fondu vyrovnávacích pamětí.

   To je důležité zejména v případě, že fond vyrovnávacích pamětí pravděpodobně podstoupí velký počet operací I/O, protože ušetří náklady na procesor spojené s opravou stránek vyrovnávacích pamětí před operací I/O a poté je zruší.
5. Existuje několik výhod pro umístění fondů vyrovnávacích pamětí nad pruhem, i když jsou dostatečně malé, aby se vešly pod pruh. Patří mezi ně:
   - 31bitové omezení virtuálního úložiště-například větší prostor pro společné úložiště.
   - Je-li třeba neočekávaně zvýšit velikost fondu vyrovnávacích pamětí v době, kdy je intenzivně využíván, dochází k menšímu dopadu a riziku pro správce front a jeho pracovní zátěž, a to přidáním více vyrovnávacích pamětí do fondu vyrovnávacích pamětí, který je již nad pruhem, než přesunutím fondu vyrovnávacích pamětí nad panel a následným přidáním více vyrovnávacích pamětí.

6. Vyladťe fond vyrovnávacích pamětí nula a fond vyrovnávacích pamětí pro krátkodobé zprávy (fond vyrovnávacích pamětí 2) tak, aby nebyla překročena prahová hodnota volného prostoru 15% (to znamená, že QPSTCBSL děleno QPSTNBUF je vždy větší než 15%). Zůstane-li více než 15% vyrovnávacích pamětí volných, lze se během normálního provozu vyvarovat vstupu/výstupu sad stránek používajících tyto fondy vyrovnávacích pamětí, i když se do sad stránek zapisují zprávy starší než dva kontrolní body.

   Upozornění: Optimální hodnota těchto parametrů závisí na charakteristice jednotlivých systémů. Uvedené hodnoty jsou určeny pouze jako vodítko a nemusí být vhodné pro váš systém.
7. SYSTÉM.* fronty, které jsou velmi hluboké, například SYSTEM.CHANNEL.SYNCQmůže mít prospěch z umístění do vlastního fondu vyrovnávacích pamětí, pokud je k dispozici dostatek paměti.

IBM MQ SupportPac MP16 - IBM MQ pro z/OS Plánování kapacity & ladění poskytuje další informace o vyladění fondů vyrovnávacích pamětí.

z/OS Plánování prostředí protokolování

Toto téma slouží k plánování počtu, velikosti a umístění protokolů a archivů protokolů používaných produktem IBM MQ.

Protokoly se používají k:

- Zapsat informace o obnově trvalých zpráv
- Zaznamenat informace o jednotkách práce pomocí trvalých zpráv
- Zaznamenejte informace o změnách objektů, jako je například definice fronty.
- Záložní struktury prostředku CF

a pro další interní informace.

Protokolovací prostředí IBM MQ je zavedeno pomocí maker systémových parametrů pro uvedení voleb, jako například: zda mít jeden nebo dva aktivní protokoly, jaká média se mají použít pro svazky protokolu archivace a kolik vyrovnávacích pamětí protokolu se má mít.

Tato makra jsou popsána v části Vytvořit datové sady zaváděcího programu a protokolu a Přizpůsobte modul systémových parametrů.

Poznámka: Používáte-li skupiny sdílení front, ujistěte se, že jste definovali datové sady zaváděcího programu a protokolu s volbou SHAREOPTIONS (2 3).

Tento oddíl obsahuje informace o následujících tématech:

z/OS *Definice datových sad protokolu*

Prostřednictvím tohoto tématu můžete rozhodnout o nejvhodnější konfiguraci pro datové sady protokolu.

Toto téma obsahuje informace, které vám pomohou odpovědět na následující otázky:

- Měla by vaše instalace používat jednoduché nebo duální protokolování?
- Kolik datových sad aktivního protokolu potřebujete?
- “Jak velké by měly být aktivní protokoly?” na stránce 160
- Umístění aktivního protokolu
- “Šifrování aktivního protokolu s šifrováním datové sady z/OS” na stránce 161

Měla by vaše instalace používat jednoduché nebo duální protokolování?

Obecně byste měli používat duální protokolování pro výrobu, abyste minimalizovali riziko ztráty dat. Chcete-li, aby váš testovací systém odrážel produkci, měly by oba používat duální protokolování, jinak by vaše testovací systémy mohly používat jedno protokolování.

S jedním protokolováním se data zapisují do jedné sady datových sad protokolu. S duálními daty protokolování se zapisují do dvou sad datových sad protokolu, takže v případě problému s jednou datovou sadou protokolu, jako je například nechtěně odstraněná datová sada, lze k obnově dat použít ekvivalentní datovou sadu v druhé sadě protokolů.

S duálním protokolováním vyžadujete dvakrát více DASD než s jedním protokolováním.

Pokud používáte duální protokolování, použijte také duální BSDS a duální archivaci, abyste zajistili odpovídající zajištění obnovy dat.

Duální aktivní protokolování zvyšuje malé náklady na výkon.

Upozornění: Použití technologií zrcadlení disku, jako je Metro Mirror, nemusí být nutně náhradou za duální protokolování a duální BSDS. Dojde-li k nechtěnému odstranění zrcadlené datové sady, dojde ke ztrátě obou kopií.

Používáte-li trvalé zprávy, může jednotlivé protokolování zvýšit maximální kapacitu o 10-30% a také zlepšit dobu odezvy.

Jedno protokolování používá datové sady aktivního protokolu 2-310, zatímco duální protokolování používá datové sady aktivního protokolu 4-620 k zajištění stejného počtu aktivních protokolů. Proto jednoduché protokolování snižuje množství protokolovaných dat, což může být důležité, pokud je vaše instalace omezena na I/O.

Kolik datových sad aktivního protokolu potřebujete?

Počet protokolů závisí na aktivitách správce front. Pro testovací systém s nízkou propustností mohou být vhodné tři datové sady aktivního protokolu. V případě produkčního systému s vysokou propustností můžete požadovat maximální počet dostupných protokolů, takže pokud dojde k problému s odlehčováním protokolů, máte více času na vyřešení problémů.

Musíte mít alespoň tři datové sady aktivního protokolu, ale je vhodnější definovat více. Je-li například pravděpodobné, že doba potřebná k vyplnění protokolu se blíží době nutné k archivaci protokolu během špičkového zatížení, definujte další protokoly.

Poznámka: Sady stránek a datové sady aktivního protokolu jsou vhodné k umístění v části EAS (extended address space) svazků s rozšířenou adresou (EAV) a datová sada protokolu archivu může být také umístěna v EAS.

Měli byste také definovat více protokolů pro odsazení možných prodlev v archivaci protokolu. Pokud používáte archivní protokoly na pásce, věnujte čas potřebný pro připojení pásky.

Zvažte možnost mít dostatek aktivního protokolovacího prostoru pro uchování dat v hodnotě jednoho dne v případě, že systém nemůže provést archivaci kvůli nedostatku DASD nebo protože nemůže zapisovat na pásku. Pokud se zaplní všechny aktivní protokoly, produkt IBM MQ nebude moci zpracovat trvalé zprávy nebo transakce. Je velmi důležité mít dostatek aktivního prostoru pro žurnál.

Je možné dynamicky definovat nové datové sady aktivního protokolu jako způsob minimalizace efektu prodlev nebo problémů archivu. Nové datové sady lze rychle uvést do stavu online pomocí příkazu **DEFINE LOG** , aby se vyhnuli "stall" správce front kvůli nedostatku místa v aktivním protokolu.

Chcete-li definovat více než 31 datových sad aktivního protokolu, musíte nakonfigurovat prostředí protokolování tak, aby používalo formát BSDS verze 2. Po použití formátu BSDS verze 2 lze pro každý svazek kopií protokolu definovat až 310 datových sad aktivního protokolu. Informace o převodu na formát BSDS verze 2 naleznete v části “Plánování zvýšení maximálního rozsahu adresovatelných protokolů” na stránce 168 .

Můžete určit, zda váš správce front používá BSDS verze 2 nebo vyšší, a to buď spuštěním obslužného programu mapy protokolu tisku (CSQJU004), nebo ze zprávy CSQJ034I vydané během inicializace správce front. Konec rozsahu RBA protokolu FFFFFFFFFFFFFFFFve zprávě CSQJ034I označuje, že se používá formát BSDS verze 2 nebo vyšší. Konec rozsahu RBA protokolu 0000FFFFFFFFFFFFve zprávě CSQJ034I označuje, že se používá BSDS ve formátu verze 1.

Pokud správce front používá formát BSDS verze 2 nebo vyšší, je možné použít příkaz **DEFINE LOG** k dynamickému přidání více než 31 datových sad aktivního protokolu do kruhu kopie protokolu.

Jak velké by měly být aktivní protokoly?

V systému IBM MQ 8.0je maximální podporovaná velikost aktivního protokolu při archivaci na disk 4 GB. V předchozích vydáních produktu je maximální podporovaná velikost aktivního protokolu při archivaci na disk 3 GB.

Při archivaci na pásku je maximální velikost aktivního protokolu 4 GB.

Měli byste vytvořit aktivní protokoly o velikosti alespoň 1 GB pro produkční a testovací systémy.

Důležité: Při přidělování datových sad musíte být opatrní, protože IDCAMS zaokrouhluje velikost, kterou přidělíte.

Chcete-li přidělit protokol o velikosti 3 GB, zadejte jednu z následujících voleb:

- Válce (4369)
- Megabajty (3071)
- TRACKS (65535)
- ZÁZNAM (786420)

Libovolné z těchto přidělení 2.99995 GB.

Chcete-li přidělit protokol 4GB , zadejte jednu z následujících voleb:

- Válce (5825)
- Megabajty (4095)
- SKLADBY (87375)
- ZÁZNAM (1048500)

Libovolné z těchto přidělení 3.9997 GB.

Při použití rozložených datových sad, kde je datová sada rozložena na více svazků, je uvedená hodnota velikosti přidělena na každém svazku DASD použitém pro rozložení. Chcete-li tedy použít 4 GB protokoly a čtyři svazky pro rozložení, měli byste uvést:

- CYLinders (1456)
- Megabajty (1023)

Nastavení těchto atributů přidělí 4 * 1456 = 5824 Cylinders nebo 4 * 1023 = 4092 megabajtů.

Poznámka: Rozložení je podporováno při použití datových sad s rozšířeným formátem. Toto je obvykle nastaveno správcem datových úložišť.

Informace o provádění procedury viz Zvýšení velikosti aktivního protokolu .

Umístění aktivního protokolu

Měli byste spolupracovat se svým týmem správy úložišť na nastavení fondů úložišť pro správce front. Je třeba zvážit:

- Konvence pojmenování, takže správci front používají správné definice SMS.
- Prostor požadovaný pro aktivní a archivní protokoly. Fond úložišť by měl mít dostatek prostoru pro aktivní protokoly z celého dne.
- Výkon a odolnost vůči selháním.

Z důvodů výkonu byste měli zvážit rozložení datových sad aktivního protokolu. Operace I/O je rozložena na více svazků a zkracuje dobu odezvy I/O, což vede k vyšší propustnosti. Informace o přidělení velikosti aktivních protokolů při použití rozložení naleznete v předchozím textu.

Měli byste zkontrolovat statistiku I/O pomocí sestav z produktu RMF nebo podobného produktu. Provádějte přezkoumání těchto statistik měsíčně (nebo častěji) pro datové sady IBM MQ , abyste se ujistili, že kvůli umístění datových sad nedochází k žádným prodlevám.

V některých situacích může být velký počet operací I/O sady stránek IBM MQ , což může mít vliv na výkon protokolu IBM MQ , pokud jsou umístěny na stejném serveru DASD.

Používáte-li duální protokolování, ujistěte se, že každá sada aktivních a archivních protokolů je od sebe oddělena. Například je alokujte na oddělených subsystémech DASD nebo na různých zařízeních.

To snižuje riziko jejich ztráty, pokud je jeden ze svazků poškozený nebo zničený. Pokud jsou ztraceny obě kopie protokolu, pravděpodobnost ztráty dat je vysoká.

Když vytváříte nová data aktivního protokolu, měli byste je předformátovat pomocí CSQJUFMT. Pokud protokol není předformátován, správce front jej při prvním použití formátuje, což má vliv na výkon.

U starších DASD s velkými spinning disky jste museli být opatrní, které svazky byly použity, abyste získali nejlepší výkon.

Díky modernímu DASD, kde jsou data rozložena na mnoha discích o velikosti PC, se nemusíte tolik obávat, které svazky se používají.

Váš správce datových úložišť by měl kontrolovat podnikový DASD, aby přezkoumal a vyřešil případné problémy s výkonem. Chcete-li získat dostupnost, můžete použít jednu sadu protokolů na jednom subsystému DASD a duální protokoly na jiném subsystému DASD.

Šifrování aktivního protokolu s šifrováním datové sady z/OS

Funkci šifrování datové sady z/OS můžete použít na datové sady aktivního protokolu pro správce front spuštěné na serveru IBM MQ for z/OS 9.1.4 nebo novějším.

Tyto datové sady aktivního protokolu musíte přidělit pomocí atributů EXTENDED a popisku klíče datové sady, který zajišťuje, že jsou data šifrována pomocí AES.

Viz část důvěrnost pro data v klidu na systému IBM MQ for z/OS se šifrováním datové sady. Další informace viz.

z/OS *Použití funkce MetroMirror s IBM MQ*

IBM Metro Mirror, dříve známé jako PPRC (Synchronous Peer to Peer Remote Copy), je řešení synchronní replikace mezi dvěma úložnými subsystémy, kde jsou dokončeny operace zápisu na primárním i sekundárním svazku před tím, než je operace zápisu považována za dokončenou. Funkci Metro Mirror lze použít v prostředích, která nevyžadují žádnou ztrátu dat v případě selhání úložného subsystému.

Podporované typy datových sad

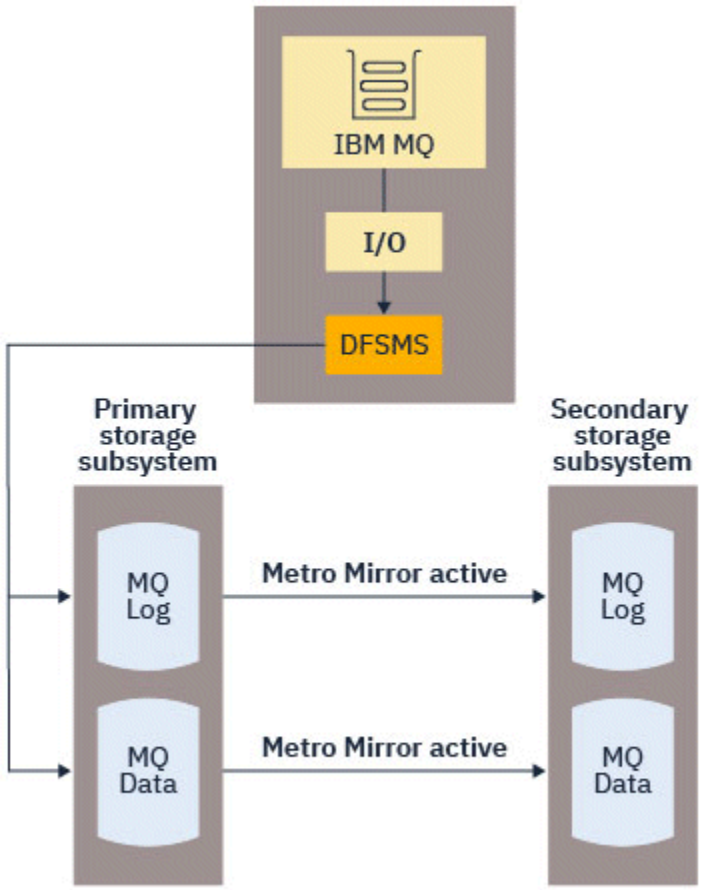
Všechny následující typy datových sad IBM MQ lze replikovat pomocí funkce Metro Mirror. Avšak přesně ty, které jsou replikovány, závisí na požadavcích na dostupnost vašeho podniku:

- Aktivní protokoly
- Protokol archivace
- zaváděcí datová sada
- Sady stránek
- Datová sada sdílených zpráv (SMDS)
- Datové sady používané pro konfiguraci, například na kartách CSQINP* DD v MSTR JCL

Použití aktivních protokolů zHyperWrite with IBM MQ

Když se provede zápis do datové sady, která se replikuje pomocí funkce Metro Mirror, zápis se nejprve provede na primární svazek a pak se replikuje na sekundární svazek. Tato replikace je prováděna úložným subsystémem a je transparentní pro aplikaci, která vydala zápis, například IBM MQ.

Tento proces je znázorněn v následujícím diagramu.

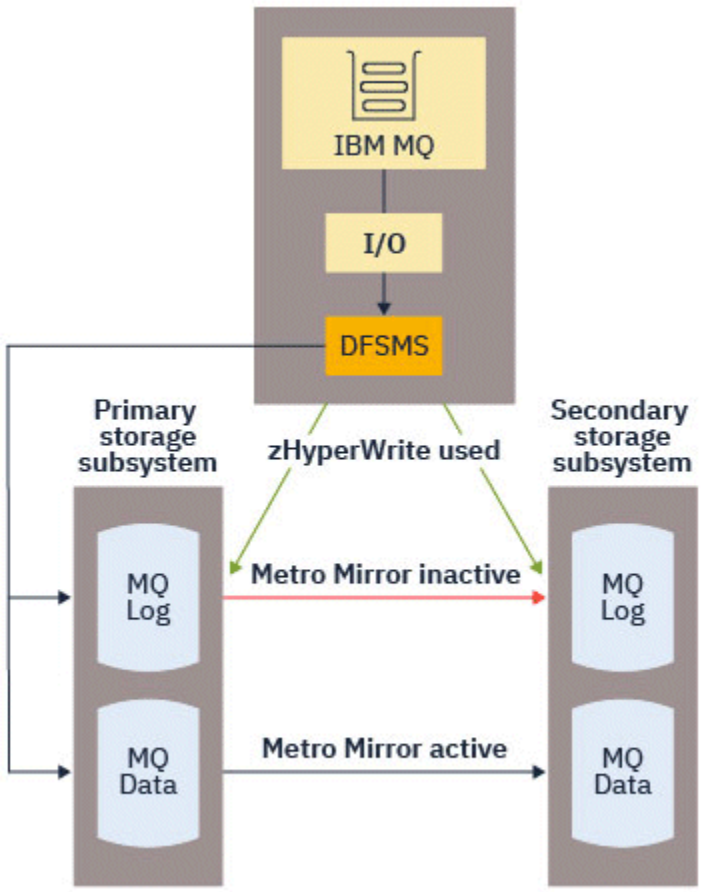


Protože oba zápisy do primárních a sekundárních úložných subsystémů musí být dokončeny před návratem zápisu do produktu IBM MQ, může mít použití funkce Metro Mirror dopad na výkon. Tento dopad na výkon musíte vyvážit s výhodami dostupnosti, které přináší funkce Metro Mirror.

Aktivní protokoly IBM MQ jsou nejcitlivější na dopad použití funkce Metro Mirrorna výkon. Produkt IBM MQ umožňuje použití zHyperZápis s aktivními protokoly, což pomáhá snížit tento dopad na výkon.

zHyperZápis je technologie úložného subsystému, která pracuje s produktem z/OS , aby se snížil dopad zápisů provedených do datových sad, které jsou replikovány pomocí funkce Metro Mirrorna výkon. Když se použije volba zHyperWrite, zápis do primárních a sekundárních svazků se vydá paralelně na úrovni Data Facility Storage Management Subsystem (DFSMS), místo aby se postupně na úrovni úložného subsystému, čímž se sníží dopad na výkon.

Následující diagram ilustruje zHyperZápis používaný pro aktivní protokoly a Metro Mirror používaný pro ostatní typy datových sad IBM MQ . Všimněte si, že pokud zápis zHyperselže, DFSMS transparentně znovu vydá zápis pomocí funkce Metro Mirror.



zHyperZapsat IBM MQje podporován pouze na datových sadách aktivního protokolu.

Chcete-li použít příkaz zHyperWrite s aktivními protokoly, musíte:

- Nakonfigurujte IBM MQ pro použití zápisu zHypera
- Aktivní protokoly musí být na svazcích s možností zápisu zHyper

Produkt IBM MQ můžete nakonfigurovat tak, aby používal zápis zHyper, pomocí jedné z následujících metod:

- V modulu systémových parametrů zadejte hodnotu ZHYWRITE(YES).
- Zadejte příkaz SET LOG ZHYWRITE(YES).

Nastavte následující podmínky pro datové sady aktivního protokolu, aby byly na svazcích s možností zápisu zHyper:

- Povolte svazky pro funkci Metro Mirrora svazky podporují funkci zHyperWrite
- Ujistěte se, že svazky mají povolenou funkci HyperSwap
- Uveďte HYPERWRITE=YES v parametru IECIOSxx

V 9.3.5 Před IBM MQ 9.3.5, pokud jsou splněny všechny předchozí podmínky, pak jsou pro zápis zHyperpovoleny zápisy do aktivních protokolů. Pokud není splněna jedna nebo více z těchto podmínek, produkt IBM MQ zapisuje do aktivních protokolů jako obvykle a funkce Metro Mirror replikuje zápisy, je-li konfigurována.

V 9.3.5 V systému IBM MQ 9.3.5, pokud je uvedeno ZHYWRITE (YES), pak se IBM MQ vždy pokusí použít zHyperZapsat při zápisu do aktivních protokolů, bez ohledu na to, zda jsou protokoly na svazcích schopných zápisu zHyper. Pokud protokoly nejsou na svazcích schopných zápisu zHyper, pak funkce Metro

Mirror replikuje zápisy, je-li konfigurována. Neexistují žádné negativní účinky pokusu o použití zápisu zHyper, pokud protokoly nejsou na svazcích s možností zápisu zHyper.

Notes:

- Produkt IBM MQ nevyžaduje, aby všechny datové sady aktivního protokolu byly na svazcích s možností zápisu zHyper.

  Pokud produkt IBM MQ zjistí, že některé datové sady aktivního protokolu jsou na svazcích s možností zápisu zHyper, a jiné ne, vydá zprávu CSQJ166E a pokračuje ve zpracování.
- IBM MQ kontroluje, zda jsou datové sady aktivního protokolu zHyperschopné zápisu při prvním otevření datových sad.

  Datové sady protokolu se otevírají buď při spuštění správce front, nebo při dynamickém přidávání pomocí příkazu DEFINE LOG. Pokud jsou datové sady protokolu zHyperschopné zápisu, zatímco je správce front má otevřené, správce front to nezjistí, dokud nebude restartován.

Výstup příkazu DISPLAY LOG můžete použít k označení, zda jsou aktuální datové sady aktivního protokolu zHyperschopné zápisu. Následující příklad ukazuje, že obě datové sady jsou schopné zápisu zHyper. Pokud byl správce front konfigurován s volbou ZHYWRITE (YES), budou pro zápis zHyperpovoleny zápisy do těchto protokolů:

```
Copy %Full zHyperWrite DSName
 1      4  CAPABLE     MQTST.SUBSYS.MQDL.LOGCOPY1.DS001
 2      4  CAPABLE     MQTST.SUBSYS.MQDL.LOGCOPY2.DS001
```

z/OS *Plánování archivního úložiště protokolu*

Prostřednictvím tohoto tématu můžete porozumět různým způsobům správy datových sad protokolu archivu.

Datové sady protokolu archivace můžete umístit na pásky se standardním popiskem nebo na DASD a můžete je spravovat pomocí správce datových úložišť DFHSM (Data Facility Hierarchical Storage Manager). Každý logický záznam z/OS v datové sadě archivního protokolu je řídicí interval VSAM z datové sady aktivního protokolu. Velikost bloku je násobkem 4 kB.

Datové sady protokolu archivu jsou dynamicky přidělovány s názvy zvolenými pomocí IBM MQ. Předpona názvu datové sady, velikost bloku, název jednotky a velikosti DASD potřebné pro taková přidělení jsou uvedeny v modulu parametrů systému. V době instalace můžete také zvolit, aby produkt IBM MQ přidal k názvu datové sady protokolu archivace datum a čas.

Není možné zadat s IBM MQ, specifickými svazky pro nové archivní protokoly, ale ke správě tohoto můžete použít rutiny správy úložiště. Dojde-li k chybám přidělení, odloží se odlehčování až do příštího spuštění odlehčování.

Zadáte-li duální protokoly archivace v době instalace, bude každý interval řízení protokolu načtený z aktivního protokolu zapsán do dvou datových sad protokolu archivace. Záznamy protokolu, které jsou obsaženy ve dvojici datových sad protokolu archivace, jsou identické, ale body konce svazku nejsou synchronizovány pro datové sady s více svazky.

Mají být archivační protokoly uloženy na pásce nebo na DASD?

Při rozhodování, zda použít pásku nebo DASD pro protokoly archivace, je třeba zvážit několik faktorů:

- Před rozhodnutím o pásce nebo disku zkontrolujte své provozní postupy. Pokud například zvolíte archivaci na pásku, musí být v případě potřeby k dispozici dostatek páskové jednotky. Po havárii mohou všechny subsystémy požadovat páskové jednotky a nemusí mít tolik volných páskových jednotek, kolik očekáváte.
- Během obnovy jsou archivní protokoly na pásce k dispozici ihned po připojení pásky. Pokud byly použity archivy DASD a datové sady migrovány na pásku pomocí hierarchického správce datových úložišť (HSM), dojde k prodlevě, zatímco HSM opětovně vyvolá každou datovou sadu na disk. Datové sady můžete

vyvolat dříve, než se použije protokol archivace. Nicméně, není vždy možné předpovědět správné pořadí, ve kterém jsou požadovány.

- Při použití archivních protokolů na DASD, je-li požadováno mnoho protokolů (což může být případ při obnově sady stránek po obnově ze zálohy), můžete požadovat, aby velké množství DASD uchovávalo všechny archivní protokoly.
- V systému s nízkým využitím nebo v testovacím systému může být vhodnější mít archivní protokoly na DASD, aby se eliminovala potřeba připojení pásek.
- Oba příkazy RECOVER CFSTRUCT a zálohování trvalé pracovní jednotky vedou ke zpětnému čtení protokolu. Páskové jednotky s hardwarovou kompresí špatně fungují na operacích, které se čtou dozadu. Naplánujte dostatek dat protokolu na DASD, abyste se vyhnuli zpětnému čtení z pásky.

Archivace na DASD nabízí rychlejší obnovitelnost, ale je dražší než archivace na pásku. Používáte-li duální protokolování, můžete určit, že primární kopie archivního protokolu přejde na DASD a sekundární kopie na pásku. Tím se zvýší rychlost obnovy bez použití tolika zařízení DASD a pásku můžete použít jako zálohu.

Podrobnosti o tom, jak archivovat protokoly z pásky na server DASD a jak provádět reverzní proces, naleznete v části “Změna úložného média pro protokoly archivu” na stránce 166 .

Archivace na pásku

Pokud se rozhodnete archivovat na páskové zařízení, produkt IBM MQ může rozšířit na maximálně 20 nosičů.

Pokud uvažujete o změně velikosti datové sady aktivního protokolu tak, aby se sada vešla na jeden páskový nosič, všimněte si, že kopie BSDS je umístěna na stejném páskovém nosiči jako kopie datové sady aktivního protokolu. Upravte velikost datové sady aktivního protokolu směrem dolů, abyste posunutili prostor požadovaný pro BSDS na páskovém nosiči.

Pokud použijete duální archivní protokoly na pásce, je typické, že jedna kopie bude zadržena lokálně, a druhá kopie bude zadržena mimo pracoviště pro použití při zotavení z havárie.

Archivace na svazky DASD

Produkt IBM MQ vyžaduje, abyste katalogizili všechny datové sady protokolu archivace přidělené na jiných než páskových zařízeních (DASD). Pokud se rozhodnete archivovat na DASD, parametr CATALOG makra CSQ6ARVP musí mít hodnotu YES. Pokud je tento parametr NO a rozhodnete se umístit datové sady protokolu archivace na DASD, obdržíte zprávu CSQJ072E pokaždé, když je přidělena datová sada protokolu archivace, ačkoli IBM MQ stále katalogizuje datovou sadu.

Je-li datová sada protokolu archivace zadržena na serveru DASD, datové sady protokolu archivace se mohou rozšířit na jiný svazek; více svazků je podporováno.

Pokud se rozhodnete použít DASD, ujistěte se, že přidělení primárního prostoru (množství i velikost bloku) je dostatečně velké, aby obsahovalo buď data přicházející z datové sady aktivního protokolu, nebo data z odpovídajícího BSDS, podle toho, která z nich je větší.

Tím se minimalizuje možnost nechtěných kódů z/OS X'B37' nebo X'E37' nestandardního ukončení během procesu odlehčování. Alokace primárního prostoru je nastavena pomocí parametru PRIQTY (primární množství) makra CSQ6ARVP .

Datové sady protokolu archivace mohou existovat ve velkých datových sadách nebo v sekvenčních datových sadách s rozšířeným formátem. Rutiny SMS ACS nyní používají DSNTYPE (LARGE) nebo DSNTYPE (EXT).

Produkt IBM MQ podporuje alokaci protokolů archivu jako datových sad rozšířeného formátu. Když se použije rozšířený formát, maximální velikost protokolu archivace se zvýší z 65535 stop na maximální velikost aktivního protokolu 4GB. Archivní protokoly jsou způsobilé pro přidělení v rozšířeném adresním prostoru (EAS) svazků rozšířené adresy (EAV).

Tam, kde jsou k dispozici požadované úrovně hardwaru a softwaru, může přidělení archivních protokolů do datové třídy definované pomocí COMPACTION s použitím zEDC snížit diskové úložiště požadované pro uchování archivních protokolů. Další informace viz IBM MQ for z/OS: Snížení

obsazenosti úložiště pomocí produktu IBM zEnterprise Data Compression (zEDC) a zEnterprise Data Compression (zEDC) .

Funkci šifrování datové sady z/OS lze použít na protokoly archivu pro správce front spuštěné v systému IBM MQ. Tyto archivní protokoly musí být přiděleny prostřednictvím rutin ACS (Automatic Class Selection) do datové třídy definované pomocí atributů EXTENDED a popisku klíče datové sady, který zajišťuje, že data jsou šifrována pomocí AES.

Použití SMS s datovými sadami protokolu archivace

Máte-li nainstalovaný MVS/DFP subsystém správy úložišť (DFSMS), můžete napsat filtr ACS (Automatic Class Selection) pro datové sady protokolu archivace, který vám pomůže je převést do prostředí SMS.

Takový filtr může například směrovat výstup do datové sady DASD, kterou může spravovat DFSMS . Při použití filtru ACS tímto způsobem je třeba postupovat opatrně. Protože SMS vyžaduje katalogizaci datových sad DASD, musíte se ujistit, že pole CATALOG DATA makra CSQ6ARVP obsahuje hodnotu YES. Pokud se tak nestane, vrátí se zpráva CSQJ072E . Datová sada je však stále katalogizována produktem IBM MQ.

Další informace o filtrech ACS viz Datové sady, které DFSMShsm dynamicky přiděluje během zpracování agregované zálohy.

z/OS *Změna úložného média pro protokoly archivu*

Procedura pro změnu úložného média používaného protokoly archivu.

Informace o této úloze

Tato úloha popisuje, jak změnit úložné médium používané pro protokoly archivace, například přechod z archivace na pásku na archivaci na DASD.

Máte na výběr, jak provést změny:

1. Změny proveďte pouze pomocí makra CSQ6ARVP , aby byly použity při příštím spuštění správce front.
2. Proveďte změny pomocí makra CSQ6ARVP a dynamicky pomocí příkazu SET ARCHIVE . To znamená, že změny se použijí od doby, kdy správce front příště archivuje soubor protokolu, a po restartování správce front přetrvají.

Postup

1. Změna tak, aby archivní protokoly byly uloženy na DASD místo na pásce:
   a) Přečtěte si sekci “Archivace na svazky DASD” na stránce 165 a zkontrolujte parametry CSQ6ARVP .
   b) Proveďte změny v následujících parametrech v souboru CSQ6ARVP .
      - Aktualizujte parametry UNIT a v případě potřeby parametry UNIT2 .
      - Aktualizujte parametr BLKSIZE, protože optimální nastavení pro DASD se liší od pásky.
      - Nastavte parametry PRIQTY a SECQTY tak, aby byly dostatečně velké, aby pojaly největší z aktivních protokolů nebo BSDS.
      - Nastavte parametr CATALOG na hodnotu YES.
      - Potvrďte, že nastavení ALCUNIT je to, co chcete. Měli byste použít BLK, protože je nezávislá na typu zařízení.
      - Nastavte parametr ARCWTOR na hodnotu NO, pokud ještě není.
2. Změna tak, aby archivní protokoly byly uloženy na pásce místo DASD:
   a) Přečtěte si sekci “Archivace na pásku” na stránce 165a zkontrolujte parametry CSQ6ARVP .
   b) Proveďte změny následujících parametrů v souboru CSQ6ARVP:
      - Aktualizujte parametry UNIT a v případě potřeby parametry UNIT2 .

- Aktualizujte parametr BLKSIZE, protože optimální nastavení pásky se liší od DASD.
- Potvrďte, že nastavení ALCUNIT je to, co chcete. Měli byste použít BLK, protože je nezávislá na typu zařízení.
- Zkontrolujte nastavení parametru ARCWTOR.

z/OS *Jak dlouho musím uchovávat archivní protokoly*

Informace v této části vám pomohou naplánovat strategii zálohování.

Pomocí parametru ARCRETN v části USING CSQ6ARVP nebo příkazu SET SYSTEM můžete určit, jak dlouho mají být archivační protokoly uchovávány ve dnech. Po tomto období mohou být datové sady odstraněny produktem z/OS.

Datové sady protokolu archivace můžete odstranit ručně, pokud již nejsou potřeba.

- Správce front může potřebovat protokoly archivu pro zotavení.

  Správce front může v systému BSDS uchovávat pouze posledních 1000 archivů. Pokud protokoly archivu nejsou v systému BSDS, nelze je použít pro zotavení a používají se pouze pro účely auditu, analýzy nebo typu přehrání.
- Možná budete chtít uchovat protokoly archivu, abyste mohli extrahovat informace z protokolů. Například extrahování zpráv z protokolu a kontrola, které ID uživatele zprávu vložilo nebo získalo.

Služba BSDS obsahuje informace o protokolech a dalších informacích o zotavení. Tato datová sada má pevnou velikost. Když počet protokolů archivace dosáhne hodnoty MAXARCH v CSQ6LOGP, nebo když se naplní BSDS, nejstarší informace protokolu archivace se přepíší.

Existují obslužné programy pro odebrání položek protokolu archivace z BSDS, ale obecně platí, že BSDS obtéká a překrývá nejstarší záznam protokolu archivace.

Kdy je potřeba protokol archivace

Sady stránek je třeba pravidelně zálohovat. Frekvence záloh určuje, které archivní protokoly jsou potřebné v případě ztráty sady stránek.

Je třeba pravidelně zálohovat struktury CF. Frekvence záloh určuje, které protokoly archivu jsou potřebné v případě ztráty dat ve struktuře prostředku CF.

Protokol archivace může být zapotřebí pro zotavení. Následující informace vysvětlují, kdy může být zapotřebí protokol archivace, kde jsou problémy s různými prostředky IBM MQ .

Ztráta sady stránek

Je třeba obnovit systém ze zálohy a restartovat správce front.

Potřebujete protokoly z doby, kdy byla záloha vytvořena, a také až tři datové sady protokolu před provedením zálohy.

Všechny oblasti LPAR ztratí připojitelnost ke struktuře prostředku CF nebo je struktura nedostupná.

Pomocí příkazu RECOVER CFSTRUCT obnovte strukturu.

Zotavení struktury vyžaduje protokoly od všech správců front, kteří ke struktuře přistupovali od poslední zálohy (zpět do doby, kdy byla záloha vytvořena), a zálohu struktury samotné v protokolu správce front, který zálohu vytvořil.

Pokud jste prováděli časté zálohování struktur prostředku CF, data by měla být v aktivních protokolech a neměli byste potřebovat archivní protokoly.

Pokud není k dispozici žádná nedávná záloha struktury prostředku CF, může být nutné archivovat protokoly.

Poznámka: Všechny dočasné zprávy budou ztraceny; všechny trvalé zprávy budou znovu vytvořeny provedením následujících úloh:

1. Čtení poslední zálohy struktury prostředku CF z protokolu
2. Čtení protokolů ze všech správců front, kteří použili strukturu

3. Sloučení aktualizací od zálohování

Znovusestavení administrativní struktury

Potřebujete-li znovu sestavit administrativní strukturu, budou informace načteny z posledního kontrolního bodu protokolu pro každého správce front v rámci skupiny sdílení front.

Není-li správce front aktivní, načte protokol jiný správce front v rámci skupiny sdílení front.

Protokoly archivu byste neměli potřebovat.

Ztráta datové sady SMDS

Pokud ztratíte datovou sadu SMDS nebo dojde k poškození datové sady, datová sada se stane nepoužitelnou a její stav bude nastaven na SELHÁNÍ. Struktura prostředku CF se nezměnila.

Chcete-li obnovit datovou sadu SMDS, musíte:

1. předefinovat datovou sadu SMDS a
2. Obnovte strukturu prostředku CF zadáním příkazu RECOVER CFSTRUCT .

   Poznámka: Všechny dočasné zprávy ve struktuře prostředku CF budou ztraceny. Všechny trvalé zprávy budou obnoveny.

Požadavek na protokoly správce front je stejný jako požadavek na zotavení ze struktury, která není k dispozici.

z/OS *Plánování zvýšení maximálního rozsahu adresovatelných protokolů*

Maximální rozsah adresovatelných protokolů můžete zvýšit konfigurací správce front tak, aby používal větší adresu RBA (log relative byte address).

Velikost RBA protokolu byla zvýšena z IBM MQ for z/OS 8.0. Přehled této změny naleznete v tématu Větší adresa relativního bajtu protokolu.

V 9.3.0 Správci front vytvoření v produktu IBM MQ 9.3.0 nebo novějším mají standardně povolený 8bajtový protokol RBA, a proto nevyžadují převod.

Správce front můžete kdykoli převést tak, aby používal 8bajtové hodnoty RBA protokolu. Skupina sdílení front může obsahovat některé správce front s povoleným 8bajtovým protokolem RBA a některé správce front s 6bajtovým protokolem RBA.

Zrušení změny

Změnu nelze zálohovat.

Jak dlouho to trvá?

Změna vyžaduje restart správce front. Zastavte správce front, spusťte obslužný program CSQJUCNV pro datovou sadu samozavedení (BSDS) nebo datové sady, abyste vytvořili nové datové sady, přejmenujte tyto datové sady samozavedení a restartujte správce front. Spuštění obslužného programu CSQJUCNV obvykle trvá několik sekund.

Jaký dopad to má?

- Při použití 8bajtového protokolu RBA má každý zápis dat do datových sad protokolu další bajty. Proto pro pracovní zátěž sestávající z trvalých zpráv dochází k malému nárůstu objemu dat zapsaných do protokolů.
- Data zapsaná do sady stránek nebo struktury prostředku Coupling Facility (CF) nejsou ovlivněna.

Související úlohy

Implementace větší relativní bajtové adresy protokolu

z/OS Plánování inicializátoru kanálu

Inicializátor kanálu zajišťuje komunikaci mezi správci front a spouští se ve vlastním adresním prostoru.

Existují dva typy připojení:

1. Připojení aplikací ke správci front prostřednictvím sítě. Tyto kanály jsou známé jako kanály klienta.
2. Připojení správce front ke správci front. Tyto kanály jsou známé jako kanály MCA.

Moduly listener

Program listeneru kanálu naslouchá příchozím síťovým požadavkům a v případě potřeby spustí příslušný kanál. Ke zpracování příchozích připojení potřebuje iniciátor kanálu nakonfigurovanou alespoň jednu úlohu modulu listener IBM MQ . Modul listener může být buď modul listener TCP, nebo modul listener LU 6.2 .

Každý modul listener vyžaduje port TCP nebo název LU.

Všimněte si, že pro každý inicializátor kanálu můžete mít více než jeden modul listener.

TCP/IP

Inicializátor kanálu může pracovat s více než jedním zásobníkem TCP na stejném obrazu z/OS . Například jeden zásobník TCP může být pro interní připojení a další zásobník TCP pro externí připojení.

Při definování výstupního kanálu postupujte takto:

1. Nastavíte cílového hostitele a port připojení. Může se jednat o:
   - adresa IP, například `10.20.4.6`
   - název hostitele, například `mvs-prod.myorg.com`

   Pokud k určení místa určení použijete název hostitele, produkt IBM MQ použije k vyřešení adresy IP místa určení systém DNS (Domain Name System).
2. Pokud používáte více zásobníků TCP, můžete uvést parametr **LOCLADDR** v definici kanálu, který uvádí adresu IP zásobníku, která se má použít.

Měli byste naplánovat vysoce dostupný server DNS nebo servery DNS. Není-li server DNS k dispozici, odchozí kanály nemusí být možné spustit a pravidla ověřování kanálu, která mapují příchozí připojení pomocí názvu hostitele, nelze zpracovat.

APPC a LU 6.2

Používáte-li APPC, iniciátor kanálu potřebuje jméno LU a konfiguraci v APPC.

Skupiny sdílení front

Chcete-li poskytnout jeden obraz systému a povolit příchozímu požadavku na připojení produktu IBM MQ přejít na libovolného správce front ve skupině sdílení front, je třeba provést určitou konfiguraci. Příklad:

1. Hardwarový síťový směrovač. Tento směrovač má jednu adresu IP, kterou vidí podnik, a může směrovat počáteční požadavek na libovolného správce front připojeného k tomuto hardwaru.
2. Virtuální adresa IP (VIPA). Je uvedena celopodniková adresa IP a tuto adresu lze směrovat do libovolného zásobníku TCP v prostředí sysplex. Zásobník TCP jej pak může směrovat do libovolného naslouchacího správce front v prostředí sysplex.

Ochrana provozu IBM MQ

Produkt IBM MQ můžete nakonfigurovat tak, aby používal připojení TLS k ochraně dat na spoji. Chcete-li používat protokol TLS, musíte použít digitální certifikáty a svazky klíčů.

Musíte také pracovat s personálem na vzdáleném konci kanálu, abyste se ujistili, že máte kompatibilní definice produktu IBM MQ a kompatibilní certifikáty.

Můžete řídit, která připojení se mohou připojit k produktu IBM MQ a ID uživatele, na základě

- Adresa IP
- ID uživatele klienta
- vzdálený správce front nebo
- Digitální certifikát (viz Záznamy ověření kanálu)

Je také možné omezit klientské aplikace tím, že zajistíte, že dodají platné ID uživatele a heslo (viz Ověření připojení).

Můžete zajistit, aby inicializátor kanálu fungoval, a poté nakonfigurovat každý kanál tak, aby používal protokol TLS, a to vždy po jednom.

Monitorování inicializátoru kanálu

Existují příkazy MQSC, které poskytují informace o inicializátoru kanálu a kanálech:

- Příkaz DISPLAY CHINIT poskytuje informace o inicializátoru kanálu a aktivních modulech listener.
- Příkaz DISPLAY CHSTATUS zobrazí aktivitu a stav kanálu.

Inicializátor kanálu může také vytvářet záznamy SMF s informacemi o úlohách inicializátoru kanálu a aktivitě kanálu. Další informace viz “Plánování dat SMF inicializátoru kanálu” na stránce 171.

Inicializátor kanálu vysílá zprávy do protokolu úlohy při spuštění a zastavení kanálů. Automatizace ve vašem podniku může tyto zprávy použít k zachycení stavu. Vzhledem k tomu, že některé kanály jsou aktivní pouze několik sekund, lze vytvořit mnoho zpráv. Tyto zprávy můžete potlačit buď pomocí prostředku pro zpracování zpráv z/OS , nebo nastavením parametru **EXCLMSG** pomocí příkazu SET SYSTEM .

Konfigurace definic kanálů IBM MQ

Máte-li k sobě připojeno mnoho správců front, může být obtížné spravovat všechny definice objektů. Použití klastrování IBM MQ to může zjednodušit.

Jako úplná úložiště určíte dva správce front. Jiní správci front potřebují jedno připojení k jednomu z úložišť a jedno připojení z jednoho úložiště. V případě potřeby připojení k jiným správcům front správce front vytvoří a spustí kanály automaticky.

Pokud plánujete mít v klastru velký počet správců front, měli byste plánovat správce front, kteří budou jednat jako vyhrazená úložiště a nebudou mít žádný provoz aplikací.

Další informace viz “Plánování distribuovaných front a klastrů” na stránce 19.

Akce před konfigurací inicializátoru kanálu

1. Rozhodněte se, zda používáte TCP/IP nebo APPC.
2. Používáte-li protokol TCP, přidělte alespoň jeden port pro IBM MQ.
3. Pokud potřebujete server DNS, nakonfigurujte jej tak, aby byl v případě potřeby vysoce dostupný.
4. Používáte-li APPC, přidělte jméno LU a nakonfigurujte APPC.

Akce po nakonfigurování inicializátoru kanálu, než přejdete do produkčního prostředí

1. Naplánujte, jaká připojení budete mít:
    a. Připojení klienta ze vzdálených aplikací.

   b. Kanály MCA do a z jiných správců front. Obvykle máte kanál do a z každého vzdáleného správce front.
2. Nastavte klastrování nebo se připojte k existujícímu klastrovému prostředí.
3. Zvažte, zda potřebujete použít více zásobníků TCP, VIPA nebo externí směrovač pro dostupnost před inicializátorem kanálu.
4. Pokud plánujete používat TLS:
   a. Nastavení svazku klíčů
   b. Nastavení certifikátů
5. Pokud plánujete používat ověřování kanálu:
   a. Rozhodnout o kritériích pro mapování příchozích relací na ID uživatelů MCA
   b. Povolit reverzní vyhledávání DNS nastavením parametru správce front **REVDNS**
   c. Přezkoumejte zabezpečení. Odstraňte například výchozí kanály a zadejte ID uživatelů pouze s potřebným oprávněním v atributu **MCAUSER** pro kanál.
6. Zachyťte záznamy SMF evidence a statistiky vytvořené inicializátorem kanálu a poté je zpracujte.
7. Automatizujte monitorování zpráv protokolu úlohy.
8. V případě potřeby vyladěte síťové prostředí, abyste zlepšili propustnost. S protokolem TCP zvyšují propustnost velkých vyrovnávacích pamětí pro odesílání a příjem. Můžete vynutit, aby produkt MQ používal specifické velikosti vyrovnávací paměti TCP pomocí příkazů:

```
RECOVER QMGR(TUNE CHINTCPRBDYNSZ nnnnn)
RECOVER QMGR(TUNE CHINTCPSBDYNSZ nnnnn)
```

   který nastaví SO_RCVBUF a SO_SNDBUF pro kanály na velikost v bajtech uvedenou v souboru nnnnn.

Související pojmy

“Plánování pro vašeho správce front” na stránce 141

Při nastavování správce front by vaše plánování mělo umožnit růst správce front tak, aby splňoval potřeby vašeho podniku.

z/OS Plánování dat SMF inicializátoru kanálu

Je třeba naplánovat implementaci shromažďování dat SMF pro inicializátor kanálu.

Inicializátor kanálu vytváří dva typy záznamů:

- Statistická data s informacemi o inicializátoru kanálu a úlohách v něm obsažených.
- Data evidence kanálů s informacemi podobnými příkazu DISPLAY CHSTATUS .

Shromažďování statistických dat spustíte pomocí příkazu:

```
START TRACE(STAT) CLASS(4)
```

a zastavte jej pomocí příkazu:

```
STOP TRACE(STAT) CLASS(4)
```

Shromažďování dat monitorování účtů spustíte pomocí příkazu:

```
START TRACE(ACCTG) CLASS(4)
```

a zastavte jej pomocí příkazu:

```
STOP TRACE(ACCTG) CLASS(4)
```

Můžete řídit, které kanály mají shromážděná data evidence pro použití atributu **STATCHL** v definici kanálu nebo ve správci front.

- Pro kanály klienta musíte nastavit **STATCHL** na úrovni správce front.
- Pro automaticky definované odesílací kanály klastru můžete řídit shromažďování dat evidence pomocí atributu správce front **STATACLS** .

Výchozí hodnota **STATCHL** pro správce front je OFF. Chcete-li shromažďovat data evidence kanálů, musíte kromě spuštění trasování evidence třídy 4 změnit hodnotu parametru **STATCHL** z výchozí hodnoty ve správci front nebo v definici kanálu.

Záznamy SMF se vytvoří, když:

- V 9.3.0 Od IBM MQ for z/OS 9.3.0 dále uplynul časový interval označený parametry CSQ6SYSP **STATIME** nebo **ACCTIME** , nebo je-li **STATIME** nebo **ACCTIME** ve všesměrovém vysílání shromažďování dat SMF nula. Požadavky na shromažďování dat SMF pro inicializátor kanálu a správce front jsou synchronizovány.
- Je vydán příkaz `STOP TRACE(ACCTG) CLASS(4)` nebo `STOP TRACE(STAT) CLASS(4)` nebo
- Iniciátor kanálu je vypnutý. V tomto bodě se zapíší jakákoli data SMF.

Pokud se kanál zastaví během intervalu SMF, data evidence se zapíší do SMF při příštím spuštění zpracování SMF. Pokud se klient připojí, provede nějakou práci a odpojí se, pak se znovu připojí a odpojí, jsou vytvořeny dvě sady dat evidence kanálů.

Statistická data se obvykle vejdou do jednoho záznamu SMF, avšak pokud se používá velký počet úloh, může být vytvořeno více záznamů SMF.

Data evidence se shromažďují pro každý kanál, pro který jsou povolena, a obvykle se vejdou do jednoho záznamu SMF. Pokud je však aktivní velký počet kanálů, může být vytvořeno více záznamů SMF.

Náklady na shromažďování dat SMF inicializátoru kanálu jsou malé. Obvykle je nárůst využití procesoru nižší než několik procent a často se jedná o chybu měření.

Než použijete tuto funkci, musíte pracovat s programátorem systémů z/OS , abyste se ujistili, že SMF má kapacitu pro další záznamy a že změní své procesy pro extrakci záznamů SMF tak, aby zahrnovaly nová data SMF.

Pro statistická data inicializátoru kanálu je typ záznamu SMF 115 a podtyp 231.

Pro data evidence inicializátoru kanálu je typ záznamu SMF 116 a podtyp 10.

Chcete-li tato data zpracovat, můžete napsat vlastní programy, nebo můžete použít volbu SupportPac MP1B , která obsahuje program MQSMF pro tisk dat a vytváření dat ve formátu CSV (Comma Separated Values), který je vhodný pro import do listu rozložení dat.

Pokud máte problémy se zachycením dat SMF inicializátoru kanálu, další informace naleznete v tématu Řešení problémů při zachycování dat SMF pro inicializátor kanálu (CHINIT) .

Související úlohy

Interpretace statistiky výkonu IBM MQ

Odstraňování problémů s daty evidence kanálů

z/OS Plánování prostředí z/OS TCP/IP

Chcete-li dosáhnout nejlepší propustnosti v síti, musíte použít vyrovnávací paměti pro odesílání a příjem protokolu TCP/IP o velikosti 64 kB nebo větší. Díky této velikosti systém optimalizuje velikost vyrovnávací paměti.

Viz Co je dynamické určování správné velikosti pro sítě s vysokou latencí? Další informace viz.

Velikost vyrovnávací paměti systému můžete zkontrolovat pomocí následujícího příkazu Netstat, například:

```
TSO NETSTAT ALL (CLIENT csq1CHIN
```

Výsledky zobrazují mnoho informací, včetně následujících dvou hodnot:

```
ReceiveBufferSize: 0000065536
SendBufferSize: 0000065536
```

65536 je 64 kB. Pokud je velikost vyrovnávací paměti menší než 65536, musíte spolupracovat se svým síťovým týmem, abyste zvýšili hodnoty **TCPSENDBFRSIZE** a **TCPRCVBUFRSIZE** v souboru PROFILE DDName v proceduře TCPIP. Můžete například použít následující příkaz:

```
TCPCONFIG TCPSENDBFRSZE 65536 TCPRCVBUFRSIZE 65536
```

Pokud nemůžete změnit nastavení **TCPSENDBFRSIZE** nebo **TCPRCVBUFRSIZE** v rámci celého systému, obraťte se na středisko softwarové podpory společnosti IBM .

z/OS Plánování skupiny sdílení front (QSG)

Nejjednodušším způsobem implementace sdíleného prostředí front je konfigurace správce front, přidání tohoto správce front do skupiny sdílení front a přidání dalších správců front do skupiny sdílení front.

Skupina sdílení front používá tabulky Db2 k ukládání informací o konfiguraci. Existuje jedna sada tabulek používaných všemi skupinami QSGs, které sdílejí stejnou skupinu sdílení dat Db2 .

Zprávy sdílené fronty jsou uloženy ve struktuře prostředku CF (coupling facility). Každá skupina QSG má svou vlastní sadu struktur CF. Musíte nakonfigurovat struktury tak, aby vyhovovaly vašim potřebám.

Zprávy o velikosti větší než 63KB nelze uložit do prostředku CF. Pro tyto zprávy musíte použít buď datové sady sdílených zpráv (SMDS), nebo Db2 .

Profily zpráv a plánování kapacity

Měli byste porozumět profilu zpráv vaší sdílené fronty. Níže jsou uvedeny příklady faktorů, které je třeba zvážit:

- Průměrná a maximální velikost zprávy
- Typická hloubka fronty a délka fronty výjimek. Můžete například potřebovat dostatečnou kapacitu pro uchování zpráv po celý den a typická hloubka fronty je pod 100 zpráv.

Pokud se profil zprávy změní, můžete později zvýšit velikost struktur nebo implementovat SMDS.

Chcete-li být schopni zpracovat velký objem zpráv ve špičce, můžete nakonfigurovat produkt IBM MQ tak, aby odesílal zprávy do SMDS, když využití struktury dosáhne prahových hodnot určených uživatelem.

Musíte se rozhodnout, zda chcete duplexní struktury CF. Toto je řízeno definicí struktury prostředku CF v zásadě CFRM:

1. Duplexovaná struktura používá dva prostředky párování. Dojde-li k problému s jedním prostředkem CF, nedojde k přerušení služby a strukturu lze znovu sestavit na třetím prostředku CF, je-li k dispozici. Duplexní struktury mohou významně ovlivnit výkon operací ve sdílených frontách.
2. Pokud struktura není duplexovaná, problém s prostředkem CF znamená, že sdílené fronty ve strukturách v tomto prostředku CF budou nedostupné, dokud nebude možné strukturu znovu sestavit v jiném prostředku CF.

   Produkt IBM MQ lze v tomto případě nakonfigurovat tak, aby automaticky znovu sestavoval struktury v jiném prostředku CF. Trvalé zprávy budou obnoveny z protokolů správců front.

Všimněte si, že je snadné změnit definice prostředku CF.

Můžete definovat strukturu tak, aby mohla obsahovat pouze přechodné zprávy, nebo aby mohla obsahovat trvalé a přechodné zprávy.

Struktury, které mohou zadržet trvalé zprávy, musí být pravidelně zálohovány. Zálohujte struktury prostředku CF alespoň každou hodinu, abyste minimalizovali čas potřebný k obnovení struktury v případě selhání. Záloha je uložena v datové sadě protokolu správce front, který zálohu provádí.

Pokud očekáváte vysokou propustnost zpráv ve sdílených frontách, doporučuje se mít vyhrazeného správce front pro zálohování struktur prostředku CF. To zkracuje dobu potřebnou k obnovení struktur, protože z protokolů správce front je třeba číst méně dat.

Kanály

Chcete-li poskytnout jediný obraz systému pro aplikace, které se připojují k IBM MQ QSG, můžete definovat sdílené vstupní kanály. Jsou-li nastaveny, může připojení přicházející do prostředí skupiny sdílení front přejít k libovolnému správci front v rámci skupiny sdílení front.

Pro tyto kanály může být nutné nastavit síťový směrovač nebo virtuální adresu IP (VIPA).

Můžete definovat sdílené výstupní kanály. Instanci sdíleného výstupního kanálu lze spustit z libovolného správce front v rámci skupiny sdílení front.

Další informace viz Sdílené kanály .

Zabezpečení

Prostředky produktu IBM MQ chráníte pomocí externího správce zabezpečení. Používáte-li produkt RACF, mají profily produktu RACF předponu s názvem správce front. Například fronta s názvem APPLICATION.INPUT by bylo chráněno pomocí profilu ve třídě MQQUEUE s názvem `qmgrName.APPLICATION.INPUT`.

Používáte-li skupinu sdílení front, můžete i nadále chránit prostředky profily s předponou názvu správce front nebo profily s předponou názvu skupiny sdílení front. Například `qsgName.APPLICATION.INPUT`.

Měli byste se zaměřit na použití předpony profilů s názvem skupiny sdílení front, protože to znamená, že pro všechny správce front existuje jediná definice, která vám ušetří práci a zabrání neshodě v definicích mezi správci front.

Související pojmy

“Plánování pro vašeho správce front” na stránce 141
Při nastavování správce front by vaše plánování mělo umožnit růst správce front tak, aby splňoval potřeby vašeho podniku.

z/OS Plánování prostředku Coupling Facility a odlehčovacího úložného prostředí

Toto téma použijte při plánování počátečních velikostí a formátů struktur prostředku Coupling Facility (CF) a prostředí SMDS (Shared Message Data Set) nebo prostředí Db2 .

Tento oddíl obsahuje informace o následujících tématech:

- “Definování prostředků prostředku Coupling Facility” na stránce 174
  - Rozhodování o mechanizmu ukládání dat pro odlehčování
  - Plánování struktur
  - Plánování velikosti vašich struktur
  - Mapování sdílených front na struktury
- “Plánování prostředí datové sady sdílených zpráv (SMDS)” na stránce 180
- “Plánování prostředí Db2” na stránce 183

Definování prostředků prostředku Coupling Facility

Hodláte-li používat sdílené fronty, musíte definovat struktury prostředku Coupling Facility, které bude produkt IBM MQ používat ve vaší zásadě CFRM. Chcete-li to provést, musíte nejprve aktualizovat zásadu CFRM informacemi o strukturách a poté zásadu aktivovat.

Vaše instalace má pravděpodobně existující zásadu CFRM, která popisuje dostupné prostředky CF. Obslužný program pro administrativní data se používá k úpravě obsahu zásady na základě vámi zadaných textových příkazů. Do zásady musíte přidat příkazy, které definují názvy nových struktur, prostředky párování, v nichž jsou definovány, a velikost struktur.

Zásada CFRM také určuje, zda jsou struktury IBM MQ duplexovány a jak jsou realokovány ve scénářích selhání. Obnova sdílené fronty obsahuje doporučení pro konfiguraci CFRM pro odolnost vůči selháním, která mají vliv na prostředek CF.

Rozhodnutí o odlehčovacím úložném prostředí

Data zpráv pro sdílené fronty lze odlehčovat z prostředku Coupling Facility a uložit je v tabulce Db2 nebo ve spravované datové sadě systému IBM MQ nazvané *sdílená datová sada zpráv* (SMDS). Zprávy, které jsou příliš velké pro uložení v prostředku Coupling Facility (tj. větší než 63 kB), musí být vždy odlehčeny a menší zprávy mohou být volitelně odlehčeny, aby se snížilo využití prostoru prostředku Coupling Facility.

Další informace naleznete v tématu Určení voleb odlehčování pro sdílené zprávy.

Plánování vašich struktur

Skupina sdílení front (QSG) vyžaduje definování minimálně dvou struktur. První struktura, známá jako administrativní struktura, se používá ke koordinaci interní aktivity produktu IBM MQ v rámci skupiny sdílení front. V této struktuře nejsou zadržena žádná uživatelská data. Má pevný název *qsg-name*CSQ_ADMIN (kde *qsg-name* je název skupiny sdílení front). Následné struktury jsou známé jako struktury aplikací a používají se k uchování zpráv ve sdílených frontách IBM MQ . Každá struktura může obsahovat až 512 sdílených front.

Struktura aplikace s názvem *qsg-name*CSQSYSAPPL se používá pro systémové fronty. Definování této struktury je volitelné, ale je nezbytné pro použití určitých funkcí. Standardně se jedná o SYSTEM.QSG.CHANNEL.SYNCQ a SYSTEM.QSG.UR.RESOLUTION.QUEUE jsou definovány ve struktuře *qsg-name*CSQSYAPPL.

Použití více struktur

Skupina sdílení front se může připojit až k 64 strukturám prostředku Coupling Facility. Jednou z těchto struktur musí být administrativní struktura. Je-li definována, další z těchto struktur může být struktura *qsg-name*CSQSYSAPPL. Pro data zprávy můžete použít až 63 struktur (62, pokud je definován *qsg-name*CSQSYSAPPL). Můžete se rozhodnout použít více struktur aplikace z následujících důvodů:

- Máte některé fronty, které pravděpodobně obsahují velký počet zpráv, a proto vyžadují všechny prostředky celého prostředku Coupling Facility.
- Máte požadavek na velký počet sdílených front, takže musí být rozděleny mezi více struktur, protože každá struktura může obsahovat pouze 512 front.
- Sestavy produktu RMF o charakteristice použití struktury naznačují, že byste měli rozdělit fronty, které obsahuje, do více zařízení CF.
- Chcete, aby některá data fronty byla zadržena ve fyzicky jiném prostředku Coupling Facility než jiná data fronty z důvodů izolace dat.
- Obnova trvalých sdílených zpráv se provádí pomocí atributů a příkazů úrovně struktury, například BACKUP CFSTRUCT. Chcete-li zjednodušit zálohování a obnovu, můžete přiřadit fronty, které zadržují přechodné zprávy, do jiných struktur, než jsou ty, které zadržují trvalé zprávy.

Při výběru, které spojovací prostředky přidělit struktury v, zvažte následující body:

- Vaše požadavky na izolaci dat.

- Volatilita prostředku Coupling Facility (tj. jeho schopnost uchovat data v důsledku výpadku napájení).
- Nezávislost selhání mezi přistupujícími systémy a prostředkem pro spojení nebo mezi prostředky pro spojení.
- Úroveň řídicího kódu prostředku Coupling Facility (CFCC) instalovaného v prostředku Coupling Facility (IBM MQ vyžaduje úroveň 9 nebo vyšší).

Plánování velikosti vašich struktur

Správní struktura

Administrativní struktura (*qsg-name*CSQ_ADMIN) musí být dostatečně velká, aby obsahovala 1000 položek seznamu pro každého správce front ve skupině sdílení front. Při spuštění správce front je zkontrolována struktura, aby se zjistilo, zda je dostatečně velká pro počet správců front, kteří jsou aktuálně *definováni* pro skupinu sdílení front. Správci front jsou považováni za definované pro skupinu sdílení front, pokud byly přidány obslužným programem CSQ5PQSG . Pomocí příkazu MQSC DISPLAY GROUP můžete zkontrolovat, kteří správci front jsou pro skupinu definováni.

Poznámka: Při výpočtu velikosti struktury byste měli kromě počtu správců front ve skupině sdílení front povolit i velikost velkých pracovních jednotek.

Tabulka 22 na stránce 176 zobrazuje minimální požadovanou velikost administrativní struktury pro různé počty správců front definovaných ve skupině sdílení front. Tyto velikosti byly stanoveny pro strukturu prostředku Coupling Facility úrovně 14 CFCC; pro vyšší úrovně CFCC je pravděpodobně nutné, aby byly větší.

Tabulka 22. Minimální velikost administrativní struktury

Počet správců front definovaných ve skupině sdílení front	Požadované úložiště
1	6144 kB
2	6912 KB
3	7976 KB
4	8704 kB
5	9728 KB
6	10496 KB
7	11520 KB
8	12288 KB
9	13056 KB
10	14080 kB
11	14848 KB
12	15616 KB
13	16640 KB
14	17408 KB
15	18176 KB
16	19200 KB
17	19968 KB

Tabulka 22. Minimální velikost administrativní struktury (pokračování)	
Počet správců front definovaných ve skupině sdílení front	**Požadované úložiště**
18	20736 KB
19	21760 KB
20	22528 KB
21	23296 KB
22	24320 KB
23	25088 kB
24	25856 KB
25	27136 KB
26	27904 KB
27	28672 KB
28	29696 KB
29	30464 kB
30	31232 kB
31	32256 kB

Přidáte-li správce front do existující skupiny sdílení front, je možné, že se požadavek na úložiště zvýšil nad velikost doporučenou v části Tabulka 22 na stránce 176. Pokud ano, použijte následující proceduru k odhadu požadované paměti pro strukturu *qsg-name*CSQ_ADMIN:

1. Zadejte příkaz MQSC **DISPLAY CFSTATUS(CSQ_ADMIN)** pro existujícího člena skupiny sdílení front.
2. Extrahujte informace ENTSMAX pro strukturu CSQ_ADMIN.
3. Je-li tento počet menší než 1000 násobek celkového počtu správců front, které chcete definovat ve skupině sdílení front, zvyšte velikost struktury.

Aplikační struktury

Velikost struktur aplikace požadovaných pro uchování zpráv produktu IBM MQ závisí na pravděpodobném počtu a velikosti zpráv, které mají být souběžně zadrženy ve struktuře.

Graf v souboru Obrázek 42 na stránce 178 ukazuje, jak velké struktury prostředku CF byste měli nastavit tak, aby uchovávají zprávy ve sdílených frontách. Chcete-li vypočítat velikost alokace, potřebujete následující informace:

- Průměrná velikost zpráv ve frontách.
- Celkový počet zpráv, které budou pravděpodobně uloženy ve struktuře.

Vyhledejte počet zpráv na vodorovné ose. Vyberte křivku, která odpovídá velikosti zprávy, a určete požadovanou hodnotu ze svislé osy. Například pro 200 000 zpráv o délce 1 kB udává hodnotu v rozsahu 256 až 512 MB.

Produkt Tabulka 23 na stránce 178 poskytuje stejné informace v tabulkovém formátu.

Obrázek 42. Výpočet velikosti struktury prostředku Coupling Facility

Pomocí této tabulky můžete vypočítat, jak velké mají být struktury prostředku Coupling Facility:

Tabulka 23. Výpočet velikosti struktury prostředku Coupling Facility

Počet zpráv	**1 kB**	**2 kB**	**4 kB**	**8 kB**	**16 kB**	**32 kB**	**63 kB**
100	6 MB	6 MB	7 MB	7 MB	8 MB	10 MB	14 MB
1000	8 MB	9 MB	12 MB	17 MB	27 MB	48 MB	88 MB
10000	25 MB	38 MB	64 MB	115 MB	218 MB	423 MB	821 MB
100000	199 MB	327 MB	584 MB	1097 MB	2124 MB	4177 MB	8156 MB

Vaše zásada CFRM by měla obsahovat následující příkazy:

- `INITSIZE` je velikost v kB, se kterou je struktura přidělena, když se k ní připojí první správce front.
- `SIZE` je maximální velikost, které může struktura dosáhnout.
- `FULLTHRESHOLD` nastaví procentní hodnotu prahové hodnoty, při které z/OS vydá zprávu IXC585E , aby označila, že se struktura plní.

Doporučeným postupem je zajistit, aby `INITSIZE` a `SIZE` byly v rámci faktoru 2. Například s dříve určenými čísly můžete zahrnout následující příkazy:

```
STRUCTURE NAME(structure-name)
INITSIZE(value from graph in KB, that is, multiplied by 1024)
```

```
SIZE(something larger)
FULLTHRESHOLD(85)
```

```
STRUCTURE NAME(QSG1APPLICATION1)
INITSIZE(262144) /* 256 MB */
SIZE(524288)     /* 512 MB */
FULLTHRESHOLD(85)
```

Pokud využití struktury dosáhne prahové hodnoty, kde jsou vydávány varovné zprávy, je nutný zásah. Můžete použít funkci IBM MQ k blokování operací MQPUT pro některé fronty ve struktuře, abyste zabránili aplikacím v zápisu více zpráv, spuštění více aplikací pro získání zpráv z front nebo uvedení některých aplikací, které vkládají zprávy do fronty, do klidového stavu.

Alternativně můžete použít prostředky z/OS ke změně velikosti struktury na místě. Následující příkaz z/OS :

```
SETXCF START,ALTER,STRNAME=structure-name,SIZE=newsize
```

změní velikost struktury na *newsize*, kde *newsize* je hodnota, která je menší než hodnota SIZE určená v zásadě CFRM pro strukturu, ale větší než aktuální velikost prostředku Coupling Facility.

Použití struktury prostředku Coupling Facility můžete monitorovat pomocí příkazu MQSC DISPLAY CFSTATUS .

Pokud není provedena žádná akce a struktura fronty se zaplní, vrátí se aplikaci návratový kód MQRC_STORAGE_MEDIUM_FULL. Pokud se administrativní struktura naplní, přesné příznaky závisí na tom, které procesy zaznamenají chybu, ale mohou zahrnovat následující problémy:

- Žádné odpovědi na příkazy.
- Selhání správce front v důsledku problémů při zpracování potvrzení.

Struktura CSQSYSAPPL

Struktura *qsg-name*CSQSYSAPPL je struktura aplikace pro systémové fronty. Tabulka 3 ukazuje příklad odhadu velikosti dat zpráv pro výchozí fronty definované ve struktuře *qsg-name*CSQSYSAPPL.

Tabulka 24. Tabulka zobrazující použití CSQSYSAPPL proti velikosti.

***qsg-name*Použití CSQSYSAPPL**	**určení velikosti**
SYSTEM.QSG.CHANNEL.SYNCQ	2 zprávy o velikosti 500 bajtů na aktivní instanci sdíleného kanálu
SYSTEM.QSG.UR.RESOLUTION.QUEUE	1000 zpráv o velikosti 2 kB

Navrhované počáteční hodnoty definice struktury jsou následující:

```
STRUCTURE NAME(qsg-nameCSQSYSAPPL)
INITSIZE(20480)        /* 20 MB */
SIZE(30720)            /* 30 MB */
FULLTHRESHOLD(85)
```

Tyto hodnoty lze upravit v závislosti na použití sdílených kanálů a skupinových jednotek obnovy.

Mapování sdílených front na struktury

Chcete-li definovat strukturu aplikace pro IBM MQ, použijte příkaz DEFINE CFSTRUCT . Když definujete strukturu pro IBM MQ, nezahrnujte předponu názvu skupiny sdílení front do názvu struktury. Chcete-li například definovat strukturu aplikace pro IBM MQ s názvem *qsg-name*APPLICATION1 v zásadě CFRM, zadejte následující příkaz:

```
DEFINE CFSTRUCT(APPLICATION1)
```

Atribut CFSTRUCT definice fronty se používá k mapování fronty na strukturu. Zadejte název struktury prostředku CF bez předpony názvu skupiny sdílení front v tomto atributu. Například následující příkaz definuje sdílenou frontu ve struktuře APPLICATION1 :

```
DEFINE QLOCAL(myqueue) QSGDISP(SHARED) CFSTRUCT(APPLICATION1)
```

z/OS *Plánování prostředí datové sady sdílených zpráv (SMDS)*

Používáte-li skupiny sdílení front s odlehčováním SMDS, produkt IBM MQ se musí připojit ke skupině sdílených datových sad zpráv. Toto téma vám pomůže porozumět požadavkům datové sady a konfiguraci požadované pro uložení dat zprávy produktu IBM MQ .

Datová sada sdílených zpráv (popsaná klíčovým slovem SMDS) je datová sada používaná správcem front k ukládání odlehčených dat zpráv pro sdílené zprávy uložené ve struktuře prostředku Coupling Facility.

Poznámka: Při definování datových sad SMDS pro strukturu musíte mít jednu pro každého správce front.

Je-li tato forma odlehčování dat povolena, produkt **CFSTRUCT** vyžaduje přidruženou skupinu datových sad sdílených zpráv, jednu datovou sadu pro každého správce front ve skupině sdílení front. Skupina sdílených datových sad zpráv je definována pro IBM MQ pomocí parametru **DSGROUP** v definici **CFSTRUCT** . Další parametry lze použít k dodání dalších volitelných informací, jako je počet vyrovnávacích pamětí, které se mají použít, a atributy rozšíření pro datové sady.

Každý správce front může zapisovat do datové sady, kterou vlastní, ukládat data sdílených zpráv pro zprávy zapsané prostřednictvím tohoto správce front a číst všechny datové sady ve skupině.

Seznam popisující stav a atributy pro každou datovou sadu přidruženou ke struktuře je udržován interně jako součást definice **CFSTRUCT** , takže každý správce front může zkontrolovat definici a zjistit, které datové sady jsou aktuálně k dispozici.

Tyto informace o datové sadě lze zobrazit pomocí příkazu **DISPLAY CFSTATUS TYPE(SMDS)** k zobrazení aktuálního stavu a dostupnosti a pomocí příkazu **DISPLAY SMDS** k zobrazení nastavení parametrů pro datové sady přidružené k zadanému **CFSTRUCT**.

Jednotlivé sdílené datové sady zpráv jsou efektivně identifikovány kombinací názvu vlastnícího správce front (obvykle určeného pomocí klíčového slova **SMDS**) a názvu struktury **CFSTRUCT** .

Tento oddíl popisuje následující témata:

- Parametr DSGROUP
- Parametr DSBLOCK
- Charakteristika datové sady sdílených zpráv
- Správa prostoru datové sady sdílených zpráv
- Přístup ke sdíleným datovým sadám zpráv
- Vytvoření datové sady sdílených zpráv
- Aspekty výkonu a kapacity datové sady sdílených zpráv
- Aktivace datové sady sdílených zpráv

Podrobnosti o těchto parametrech viz DEFINE CFSTRUCT .

Další informace o správě sdílených datových sad zpráv naleznete v tématu Správa sdílených datových sad zpráv .

Parametr DSGROUP

Parametr **DSGROUP** v definici **CFSTRUCT** identifikuje skupinu datových sad, ve které se mají ukládat velké zprávy pro tuto strukturu. Další parametry lze použít k určení velikosti logického bloku, která se má použít pro účely přidělení prostoru, a hodnoty pro velikost fondu vyrovnávacích pamětí a volby automatického rozšíření datové sady.

Před povolením odkládání do datových sad je třeba nastavit parametr **DSGROUP** .

- Je-li v adresáři **CFLEVEL(5)** definován nový soubor **CFSTRUCT** a je-li zadána nebo předpokládána volba **OFFLOAD(SMDS)** , musí být ve stejném příkazu uveden parametr **DSGROUP** .
- Pokud se stávající **CFSTRUCT** mění tak, aby se zvětšila hodnota **CFLEVEL** na **CFLEVEL(5)** , a je-li zadána nebo předpokládána volba **OFFLOAD(SMDS)** , musí být ve stejném příkazu uveden parametr **DSGROUP** , pokud ještě není nastaven.

Parametr DSBLOCK

Prostor v každé datové sadě je přidělen frontám jako logické bloky pevné velikosti (obvykle 256 kB) určené pomocí parametru **DSBLOCK** v definici **CFSTRUCT** a poté přidělené jednotlivým zprávám jako rozsahy stránek o velikosti 4 kB (odpovídající velikosti fyzického bloku a velikosti řídicího intervalu) v rámci každého logického bloku. Velikost logického bloku také určuje maximální množství dat zprávy, která lze číst nebo zapisovat v jedné operaci I/O, což je stejné jako velikost vyrovnávací paměti pro fond vyrovnávacích pamětí SMDS.

Větší hodnota parametru **DSBLOCK** může zlepšit výkon pro velmi velké zprávy snížením počtu samostatných operací I/O. Menší hodnota však sníží velikost vyrovnávací paměti požadované pro každý aktivní požadavek. Výchozí hodnota parametru **DSBLOCK** je 256 kB, což poskytuje přiměřenou rovnováhu mezi těmito požadavky, takže uvedení tohoto parametru nemusí být obvykle nezbytné.

Charakteristiky datové sady sdílených zpráv

Sdílená datová sada zpráv je definována jako lineární datová sada VSAM (LDS). Každá odlehčená zpráva je uložena v jednom nebo více blocích v datové sadě. Uložená data jsou adresována přímo informacemi v položkách prostředku Coupling Facility, jako je například rozšířená forma virtuálního úložiště. V samotné datové sadě není uložen žádný samostatný index nebo podobné řídicí informace.

Schéma přímého adresování znamená, že pro zprávy, které se vejdou do jednoho bloku, je pro čtení nebo zápis bloku potřebná pouze jedna operace I/O. Pokud zpráva zahrnuje více než jeden blok, mohou se operace I/O pro každý blok plně překrýt, aby se minimalizovala uplynulá doba, za předpokladu, že je k dispozici dostatek vyrovnávacích pamětí.

Datová sada sdílených zpráv také obsahuje malé množství obecných řídicích informací, které se skládají ze záhlaví na první stránce, které zahrnuje informace o stavu obnovy a restartování, a oblast kontrolního bodu prostorové mapy, která se používá k uložení mapy volného prostoru bloku při normálním ukončení správce front.

Správa prostoru datové sady sdílených zpráv

Jako informace na pozadí týkající se kapacity, výkonu a provozních aspektů může být užitečné porozumět konceptům správy prostoru ve sdílených datových sadách zpráv správci front.

Volný prostor v každé datové sadě sdílených zpráv je sledován vlastním správcem front pomocí prostorové mapy, která označuje počet stránek používaných v jednotlivých logických blocích. Mapa prostoru je udržována v hlavní paměti, zatímco datová sada je otevřená a uložena v datové sadě, když je normálně zavřená. (V situacích obnovy je mapa prostoru automaticky znovu sestavena skenováním zpráv ve struktuře prostředku Coupling Facility, aby se zjistily, které stránky datových sad jsou aktuálně používány).

Při zápisu sdílené zprávy s odlehčenými daty zprávy správce front přidělí rozsah stránek pro každý blok zpráv. Pokud je pro určenou frontu částečně použit aktuální logický blok, správce front přidělí prostor počínaje další volnou stránkou v tomto bloku, jinak přidělí nový logický blok. Pokud se celá zpráva nevejde do aktuálního logického bloku, správce front rozdělí data zprávy na konci logického bloku a přidělí nový logický blok pro další blok zprávy. Toto se opakuje, dokud nebude přidělen prostor pro celou zprávu. Jakýkoli nevyužitý prostor v posledním logickém bloku je uložen jako nový aktuální logický blok fronty. Když je datová sada uzavřena normálně, všechny nepoužívané stránky v aktuálních logických blocích se vrátí do prostorové mapy před jejím uložením.

Pokud byla načtena sdílená zpráva s odloženými daty zprávy a je připravena k odstranění, správce front zpracuje požadavek na odstranění přenesením položky prostředku Coupling Facility pro danou zprávu do seznamu pro vyčištění monitorovaného správcem front, který je vlastníkem (což může být stejný správce

front). Když položky dorazí do tohoto seznamu, vlastnící správce front tyto položky přečte a odstraní a do prostorové mapy vrátí uvolněné rozsahy stránek. Po uvolnění všech použitých stránek v logickém bloku bude blok k dispozici pro opětovné použití.

Přístup ke sdíleným datovým sadám zpráv

Každá datová sada sdílených zpráv musí být ve sdíleném úložišti s přímým přístupem, které je přístupné všem správcům front ve skupině sdílení front.

Během normálního spuštění každý správce front otevře svou vlastní datovou sadu sdílených zpráv pro přístup pro čtení/zápis a otevře všechny aktivní sdílené datové sady zpráv pro ostatní správce front pro přístup jen pro čtení, aby mohl číst zprávy uložené těmito správci front. To znamená, že každé ID uživatele správce front vyžaduje alespoň přístup UPDATE ke své vlastní datové sadě sdílených zpráv a přístup READ ke všem ostatním datovým sadám sdílených zpráv pro danou strukturu.

Pokud je nutné obnovit sdílené datové sady zpráv pomocí produktu **RECOVER CFSTRUCT**, lze proces zotavení spustit z libovolného správce front ve skupině sdílení front. Správce front, který lze použít k provedení zpracování obnovy, vyžaduje přístup UPDATE ke všem datovým sadám, které může být nutné obnovit.

Vytvoření datové sady sdílených zpráv

Každá datová sada sdílených zpráv by měla být obvykle vytvořena před vytvořením nebo změnou odpovídající definice **CFSTRUCT** , aby bylo možné použít tento způsob odlehčování zpráv, protože změny definice **CFSTRUCT** se obvykle projeví okamžitě a datová sada bude vyžadována, jakmile se správce front pokusí o přístup ke sdílené frontě, která byla k této struktuře přiřazena. V modulu SCSQPROC (CSQ4SMDS) je k dispozici ukázková úloha pro alokaci a předformátování sdílené datové sady zpráv. Úloha musí být upravena a spuštěna, aby bylo možné přidělit datovou sadu sdílených zpráv pro každého správce front, který používá příkaz CFSTRUCT s parametrem OFFLOAD (SMDS).

Pokud správce front zjistí, že byla povolena podpora odlehčování, a pokusí se otevřít datovou sadu sdílených zpráv, ale dosud nebyla vytvořena, datová sada sdílených zpráv bude označena jako nedostupná. Správce front pak nebude moci ukládat žádné velké zprávy, dokud nebude vytvořena datová sada a správce front nebude upozorněn, aby operaci zopakoval, například pomocí příkazu **START SMDSCONN** .

Datová sada sdílených zpráv je vytvořena jako lineární datová sada VSAM pomocí příkazu **DEFINE CLUSTER** Access Method Services. Definice musí určovat hodnotu **SHAREOPTIONS(2 3)** , aby ji mohl otevřít jeden správce front pro přístup pro zápis a libovolný počet správců front pro čtení současně. Musí být použita výchozí velikost řídicího intervalu 4 kB. Pokud může být nutné rozšířit datovou sadu nad 4 GB, musí být definována pomocí datové třídy SMS, která má atribut rozšířené adresovatelnosti VSAM. Datová sada sdílených zpráv je způsobilá k umístění v části EAS (extended address space) svazků s rozšířenou adresou (EAV).

Každá datová sada sdílených zpráv může být buď prázdná, nebo předformátovaná na binární nuly (pomocí **CSQJUFMT** nebo podobného obslužného programu, jako je například ukázková úloha SCSQPROC (CSQ4SMDS)), před jejím počátečním použitím. Pokud je prázdný nebo pouze částečně formátovaný při otevření, správce front automaticky formátuje zbývající prostor na binární nuly.

Aspekty výkonu a kapacity datové sady sdílených zpráv

Každá datová sada sdílených zpráv se používá k ukládání odlehčených dat pro sdílené zprávy zapsané do přidruženého produktu **CFSTRUCT** správcem front, který je vlastníkem, z oblastí v rámci stejného systému. Každá zpráva, která je odlehčena, zabírá až 768 bajtů úložiště prostředku CF, které se skládá z 256 bajtů pro položku a 512 bajtů pro dva prvky záhlaví a deskriptoru. Každá odlehčená zpráva je uložena na jedné nebo více stránkách (fyzické bloky o velikosti 4 kB) v datové sadě.

Prostor datové sady požadovaný pro daný počet odlehčených zpráv lze proto odhadnout zaokrouhlením celkové velikosti zprávy (včetně deskriptoru) na další násobek 4 kB a následným vynásobením počtem zpráv.

Pokud jde o sadu stránek, je-li datová sada sdílených zpráv téměř plná, lze ji volitelně automaticky rozbalit. Výchozí chování pro toto automatické rozšíření lze nastavit pomocí parametru **DSEXPAND** v definici **CFSTRUCT** . Toto nastavení lze přepsat pro každého správce front pomocí parametru **DSEXPAND** v příkazu **ALTER SMDS** . Automatické rozšíření se spustí, když datová sada dosáhne 90% zaplnění a je potřeba více místa. Pokud je expanze povolena, ale VSAM pokus o expanzi zamítne, protože při definování datové sady nebylo zadáno žádné přidělení sekundárního prostoru, je expanze zopakována s použitím sekundární alokace 20% aktuální velikosti datové sady.

Za předpokladu, že je datová sada sdílených zpráv definována s atributem rozšířené adresovatelnosti, je maximální velikost omezena pouze aspekty VSAM na maximálně 16 TB nebo 59 svazků. Tato velikost je výrazně větší než maximální velikost 64 GB lokální sady stránek.

Aktivace datové sady sdílených zpráv

Pokud se správce front úspěšně připojil ke struktuře prostředku Coupling Facility aplikace, zkontroluje, zda tato definice struktury určuje odlehčování s použitím přidruženého parametru **DSGROUP** . Pokud ano, správce front přidělí a otevře vlastní datovou sadu sdílených zpráv pro přístup pro zápis, otevře se pro přístup pro čtení všech existujících sdílených datových sad zpráv vlastněných jinými správci front.

Je-li datová sada sdílených zpráv otevřena poprvé (před tím, než byla zaznamenána jako aktivní ve skupině sdílení front), první stránka ještě nebude obsahovat platné záhlaví. Správce front vyplní informace záhlaví, aby identifikoval skupinu sdílení front, název struktury a vlastnícího správce front.

Po dokončení záhlaví zaregistruje správce front novou datovou sadu sdílených zpráv jako aktivní a vysílá událost, která upozorní všechny ostatní aktivní správce front na novou datovou sadu.

Pokaždé, když správce front otevře datovou sadu sdílených zpráv, ověří informace v záhlaví, aby se ujistil, že je stále používána správná datová sada a že nebyla poškozena.

z/OS *Plánování prostředí Db2*

Používáte-li skupiny sdílení front, musí se produkt IBM MQ připojit k subsystému Db2 , který je členem skupiny sdílení dat. Toto téma vám pomůže porozumět požadavkům Db2 , které se používají k uchování dat IBM MQ .

Produkt IBM MQ potřebuje znát název skupiny sdílení dat, ke které se má připojit, a název subsystému Db2 (nebo skupiny Db2), ke kterému se má připojit, aby dosáhl této skupiny sdílení dat. Tyto názvy jsou uvedeny v parametru QSGDATA makra systémového parametru CSQ6SYSP (popsáno v části Použití CSQ6SYSP).

V rámci skupiny sdílení dat se sdílené tabulky Db2 používají k zadržení:

- Informace o konfiguraci pro skupinu sdílení front.
- Vlastnosti sdílených a skupinových objektů IBM MQ .
- Volitelně data týkající se odlehčených zpráv produktu IBM MQ .

Produkt IBM MQ poskytuje jedinou sadu ukázkových úloh pro definování nezbytných Db2 tabulkových prostorů, tabulek a indexů. Tyto úlohy využívají univerzální tabulkové prostory (UTS). Dřívější verze produktu měly dvě sady úloh, jednu pro UTS a jednu pro starší typy tabulkového prostoru, které byly zamítnuty nejnovějšími verzemi produktu Db2.

Produkt IBM MQ lze i nadále používat se staršími typy tabulkových prostorů, což může být vhodné v případě, že již máte existující skupinu sdílení front. Pokud však vytváříte novou skupinu sdílení front, měla by používat UTS.

Db2 V12 Úroveň funkce 508 poskytuje proces migrace bez přerušení pro migraci tabulkových prostorů s více tabulkovými tabulkovými prostory do univerzálních tabulkových prostorů. Tento přístup můžete použít k migraci tabulkových prostorů pro více tabulek používaných existujícími skupinami sdílení front do univerzálních tabulkových prostorů bez výpadku celé skupiny sdílení front.

V produktu Db2 V13použijte volbu MOVE TABLE příkazu ALTER TABLESPACE. Další informace naleznete v tématu Přesouvání tabulek z tabulkových prostorů s více tabulkami do tabulkových prostorů s rozdělením podle růstu .

Standardně produkt Db2 používá ID uživatele osoby, která spouští úlohy, jako vlastníka prostředků Db2 . Je-li toto ID uživatele odstraněno, budou odstraněny prostředky, které jsou k němu přidruženy, a tak bude tabulka odstraněna. Zvažte použití ID skupiny k vlastnit tabulky, spíše než individuální ID uživatele. To můžete provést přidáním `GROUP=groupname` na kartu JOB a uvedením `SET CURRENT SQLID='groupname'` před jakékoli příkazy SQL.

Produkt IBM MQ používá zařízení RRS Attach produktu Db2. To znamená, že můžete zadat název skupiny Db2 , ke které se chcete připojit. Výhodou připojení k názvu připojení skupiny Db2 (spíše než ke specifickému subsystému Db2) je, že se produkt IBM MQ může připojit (nebo znovu připojit) k libovolnému dostupnému subsystému Db2 v obrazu z/OS , který je členem této skupiny. Musí existovat subsystém Db2 , který je členem skupiny sdílení dat aktivní na každém obrazu systému z/OS , kde se chystáte spustit subsystém sdílení front IBM MQ , a služba RRS musí být aktivní.

Db2 úložný prostor

U většiny instalací je požadovaná velikost úložiště Db2 přibližně 20 nebo 30 válců na zařízení 3390. Chcete-li však vypočítat požadavky na úložiště, následující tabulka vám poskytne některé informace, které vám pomohou určit, kolik úložiště Db2 vyžaduje pro data produktu IBM MQ . Tabulka popisuje délku každého řádku Db2 a kdy je každý řádek přidán do příslušné tabulky Db2 nebo z ní odstraněn. Tyto informace použijte společně s informacemi o výpočtu požadavků na prostor pro tabulky Db2 a jejich indexy v příručce *Db2 for z/OS Installation Guide*.

Tabulka 25. Plánování požadavků na úložiště Db2

Db2 název tabulky	**Délka řádku**	**Řádek se přidá, když:**	**Řádek se odstraní, když:**
CSQ.ADMIN_B_QSG	252 bajtů	Do tabulky je přidána skupina sdílení front s funkcí ADD QSG obslužného programu CSQ5PQSG .	Skupina sdílení front je odebrána z tabulky pomocí funkce REMOVE QSG obslužného programu CSQ5PQSG . (Všechny řádky související s touto skupinou sdílení front jsou při odstranění záznamu skupiny sdílení front automaticky odstraněny ze všech ostatních tabulek produktu Db2 .)
CSQ.ADMIN_B_QMGR	Až 3828 bajtů	Do tabulky je přidán správce front s funkcí ADD QMGR obslužného programu CSQ5PQSG .	Správce front je odebrán z tabulky pomocí funkce REMOVE QMGR obslužného programu CSQ5PQSG .
CSQ.ADMIN_B_STRUCTURE	1454 bajtů	Je definována první definice lokální fronty určující atribut QSGDISP (SHARED), který pojmenovává dříve neznámou strukturu v rámci skupiny sdílení front.	Poslední definice lokální fronty určující atribut QSGDISP (SHARED), který pojmenovává strukturu v rámci skupiny sdílení front, je odstraněna.
CSQ.ADMIN_B_SCST	342 bajtů	Je spuštěn sdílený kanál.	Sdílený kanál se stane neaktivním.
CSQ.ADMIN_B_SSKT	254 bajtů	Je spuštěn sdílený kanál s atributem NPMSPEED (NORMAL).	Sdílený kanál, který má atribut NPMSPEED (NORMAL), se stane neaktivním.

Tabulka 25. Plánování požadavků na úložiště Db2 (pokračování)

Db2 název tabulky	Délka řádku	Řádek se přidá, když:	Řádek se odstraní, když:
CSQ.ADMIN_B_STRBACKUP	514 bajtů	Do fronty CSQ.ADMIN_B_STRUCTURE . Každý záznam je fiktivní, dokud se nespustí příkaz BACKUP CFSTRUCT, který fiktivní položky přepíše.	Řádek se odstraní z CSQ.ADMIN_B_STRUCTURE .
CSQ.OBJ_B_AUTHINFO	3400 bajtů	Je definován objekt ověřovacích informací s QSGDISP (GROUP).	Objekt ověřovacích informací s QSGDISP (GROUP) je odstraněn.
CSQ.OBJ_B_QUEUE	Až 3707 bajtů	• Je definována fronta s atributem QSGDISP (GROUP). • Je definována fronta s atributem QSGDISP (SHARED). • Otevře se modelová fronta s atributem DEFTYPE (SHAREDYN).	• Fronta s atributem QSGDISP (GROUP) je odstraněna. • Fronta s atributem QSGDISP (SHARED) je odstraněna. • Dynamická fronta s atributem DEFTYPE (SHAREDYN) je uzavřena s volbou DELETE.
CSQ.OBJ_B_NAMELIST	Až 15127 bajtů	Je definován seznam názvů s atributem QSGDISP (GROUP).	Seznam názvů s atributem QSGDISP (GROUP) je odstraněn.
CSQ.OBJ_B_CHANNEL	Až 14127 bajtů	Je definován kanál s atributem QSGDISP (GROUP).	Kanál s atributem QSGDISP (GROUP) je odstraněn.
CSQ.OBJ_B_STGCLASS	Až 2865 bajtů	Je definována paměťová třída s atributem QSGDISP (GROUP).	Paměťová třída s třídou atributů QSGDISP (GROUP) je odstraněna.
CSQ.OBJ_B_PROCESS	Až 3347 bajtů	Je definován proces s atributem QSGDISP (GROUP).	Proces s atributem QSGDISP (GROUP) je odstraněn.
CSQ.OBJ_B_TOPIC	Až 14520 bajtů	Je definován objekt tématu s atributem QSGDISP (GROUP).	Objekt tématu s atributem QSGDISP (GROUP) je odstraněn.
CSQ.EXTEND_B_QMGR	Méně než 430 bajtů	Do tabulky je přidán správce front s funkcí ADD QMGR obslužného programu CSQ5PQSG .	Správce front je odebrán z tabulky pomocí funkce REMOVE QMGR obslužného programu CSQ5PQSG .
CSQ.ADMIN_B_MESSAGES	87 bajtů	Pro velkou zprávu PUT (1 na BLOB).	Pro velkou zprávu GET (1 na BLOB).
CSQ.ADMIN_MSGS_BAUX1 CSQ.ADMIN_MSGS_BAUX2 CSQ.ADMIN_MSGS_BAUX3 CSQ.ADMIN_MSGS_BAUX4		Tyto 4 tabulky obsahují informační obsah zpráv pro velké zprávy přidané do jedné z těchto 4 tabulek pro každý objekt BLOB zprávy. BLOBS má délku až 511 kB, takže pokud je velikost zprávy větší než 711 kB, bude pro tuto zprávu existovat více objektů BLOB.	

Použití velkého počtu zpráv sdílené fronty o velikosti větší než 63 kB může mít významný dopad na výkon vašeho systému IBM MQ . Další informace viz SupportPac MP16, Plánování a vyladění kapacity pro IBM MQ for z/OS, na adrese: SupportPacs pro IBM MQ a další oblasti projektu.

z/OS Plánování zálohování a obnovy

Vývoj postupů zálohování a obnovy dat na vašem serveru je nezbytný, aby se zabránilo nákladným a časově náročným ztrátám dat. Produkt IBM MQ poskytuje prostředky pro obnovu front i zpráv do jejich aktuálního stavu po selhání systému.

Toto téma obsahuje následující sekce:

- "Postupy zpětného získávání prostředků" na stránce 186
- "Tipy pro zálohování a obnovu" na stránce 186
- "Obnova sad stránek" na stránce 189
- "Obnova struktur prostředku CF" na stránce 190
- "Dosažení specifických cílů obnovy" na stránce 190
- "Pokyny k zálohování pro ostatní produkty" na stránce 192
- "Obnova a CICS" na stránce 192
- "Obnova a IMS" na stránce 192
- "Příprava na obnovu na alternativním serveru" na stránce 192
- "Příklad aktivity zálohování správce front" na stránce 193

Postupy zpětného získávání prostředků

Pro produkt IBM MQvyvíjejte následující procedury:

- Vytvoření bodu zotavení.
- Zálohování sad stránek.
- Zálohování struktur prostředku CF.
- Obnova sad stránek.
- Obnova z podmínek nedostatku prostoru (protokoly IBM MQ a sady stránek).
- Obnova struktur prostředku CF.

Informace o těchto informacích naleznete v části Administrace IBM MQ for z/OS .

Seznamte se s postupy používanými na vašem webu pro následující:

- Obnova po selhání hardwaru nebo napájení.
- Obnova ze selhání komponenty z/OS .
- Obnova z přerušení serveru pomocí obnovy mimo pracoviště.

z/OS Tipy pro zálohování a obnovu

V tomto tématu jsou uvedeny informace o některých úlohách zálohování a obnovy.

Proces restartování správce front obnoví data do konzistentního stavu použitím informací protokolu na sady stránek. Pokud jsou sady stránek poškozené nebo nedostupné, můžete problém vyřešit pomocí záložních kopií sad stránek (pokud jsou k dispozici všechny protokoly). Pokud jsou vaše datové sady protokolu poškozené nebo nedostupné, nemusí být možné provést úplnou obnovu.

Zvažte následující body:

- Pravidelné pořizování záložních kopií
- Nezahazujte archivní protokoly, které byste mohli potřebovat

- Neměnit DDname na přidružení sady stránek

Pravidelně pořizujte záložní kopie

Bod zotavení je termín používaný k popisu sady záložních kopií sad stránek IBM MQ a odpovídajících datových sad protokolu potřebných k obnově těchto sad stránek. Tyto záložní kopie zajišťují potenciální bod restartu pro případ ztráty sady stránek (například chyby I/O sady stránek). Pokud restartujete správce front pomocí těchto záložních kopií, data v produktu IBM MQ budou konzistentní až do okamžiku, kdy byly tyto kopie pořízeny. Za předpokladu, že jsou od tohoto bodu k dispozici všechny protokoly, lze produkt IBM MQ obnovit do bodu selhání.

Čím novější jsou vaše záložní kopie, tím rychleji může produkt IBM MQ obnovit data v sadách stránek. Obnova sad stránek závisí na všech nezbytných datových sadách protokolu, které jsou k dispozici.

Při plánování obnovy je třeba určit, jak často se mají pořizovat záložní kopie a kolik úplných cyklů zálohování se má uchovávat. Tyto hodnoty vám sdělí, jak dlouho musíte uchovat datové sady protokolu a záložní kopie sad stránek pro obnovu systému IBM MQ .

Při rozhodování o tom, jak často se mají pořizovat záložní kopie, zvažte dobu potřebnou k obnovení sady stránek. Potřebný čas je určen následujícím způsobem:

- Množství protokolů, které se mají procházet.
- Doba, kterou operátorovi trvá připojení a odebrání archivních páskových nosičů.
- Doba potřebná k přečtení části protokolu potřebného pro zotavení.
- Doba potřebná k opětovnému zpracování změněných stránek.
- Úložné médium použité pro záložní kopie.
- Metoda použitá k vytvoření a obnově záložních kopií.

Obecně platí, že čím častěji budete vytvářet záložní kopie, tím méně času trvá obnova, ale tím více času je věnováno vytváření kopií.

Pro každého správce front byste měli pořídit záložní kopie následujících položek:

- Datové sady protokolu archivu
- Kopie BSDS vytvořené v době archivace
- Sady stránek
- Definice objektů
- Vaše struktury CF

Chcete-li snížit riziko ztráty nebo poškození záložních kopií, zvažte:

- Uložení záložních kopií na různých svazcích úložišť do původních kopií.
- Uložení záložních kopií na jiném místě do původních kopií.
- Vytvoření alespoň dvou kopií každé zálohy sad stránek a, pokud používáte jedno protokolování nebo jeden BSDS, dvou kopií protokolů archivu a BSDS. Pokud používáte duální protokolování nebo BSDS, vytvořte jednu kopii obou archivních protokolů nebo BSDS.

Před přesunem produktu IBM MQ do produkčního prostředí plně otestujte a zdokumentujte své procedury zálohování.

Zálohování sad stránek

Sady stránek je třeba zálohovat pravidelně. Některé podniky zálohují sady stránek dvakrát denně.

Potřebujete aktivní a archivní protokoly od zálohy, abyste mohli provést obnovu pomocí zálohy. Potřebujete dostatek dat protokolu pro přechod o čtyři kontrolní body zpět, pokud byla záloha provedena v době, kdy byl spuštěn správce front.

K zálohování sad stránek můžete použít ADRDSSU FastReplication , což lze provést i v době, kdy je správce front aktivní. Všimněte si, že musíte zajistit dostatek prostoru ve fondu úložišť.

Zálohování definic objektů

Vytvořte záložní kopie definic objektů. K tomu použijte funkci MAKEDEF funkce COMMAND obslužného programu (popsanou v tématu Použití funkce COMMAND struktury CSQUTIL).

To byste měli provést vždy, když budete pořizovat záložní kopie datových sad správce front, a zachovat nejaktuálnější verzi.

Zálohování struktur prostředku Coupling Facility

Pokud jste nastavili nějaké skupiny sdílení front, a to i v případě, že je nepoužíváte, je nutné pravidelně zálohovat struktury prostředku CF. K tomu použijte příkaz IBM MQ BACKUP CFSTRUCT . Tento příkaz můžete použít pouze na strukturách prostředku CF, které jsou definovány s atributem RECOVER (YES). Pokud některé položky prostředku CF pro trvalé sdílené zprávy odkazují na odlehčená data zpráv uložená v datové sadě sdílených zpráv (SMDS) nebo v adresáři Db2, jsou odlehčená data načtena a zálohována společně s položkami prostředku CF. Sdílené datové sady zpráv by neměly být zálohovány odděleně.

Doporučuje se provést zálohu všech struktur CF přibližně každou hodinu, abyste minimalizovali dobu potřebnou k obnovení struktury CF.

Můžete provést všechny zálohy struktury prostředku CF v jednom správci front, což má tu výhodu, že můžete omezit nárůst využití protokolu na jednoho správce front. Případně můžete provádět zálohy pro všechny správce front ve skupině sdílení front, což má výhodu rozložení pracovní zátěže v rámci skupiny sdílení front. Bez ohledu na strategii, kterou používáte, může produkt IBM MQ vyhledat zálohu a provést příkaz RECOVER CFSTRUCT od libovolného správce front ve skupině sdílení front. Pro obnovení struktury prostředku CF je třeba přistupovat k protokolům všech správců front ve skupině sdílení front.

Zálohování zásad zabezpečení zpráv

Používáte-li produkt Advanced Message Security k vytvoření zálohy zásad zabezpečení zpráv, vytvořte zálohu pomocí obslužného programu pro zásady zabezpečení zpráv (CSQ0UTIL) ke spuštění **dspmqspl** s parametrem -export, pak uložte definice zásad, které jsou výstupem, do EXPORT DD.

Měli byste vytvořit zálohu zásad zabezpečení zpráv, kdykoli budete pořizovat záložní kopie datových sad správce front, a zachovat nejaktuálnější verzi.

Nezahazujte archivní protokoly, které byste mohli potřebovat

Produkt IBM MQ může vyžadovat použití protokolů archivace během restartu. Musíte zachovat dostatek archivních protokolů, aby mohl být systém plně obnoven. Produkt IBM MQ může použít archivní protokol k obnovení sady stránek z obnovené záložní kopie. Pokud jste tento protokol archivace zrušili, produkt IBM MQ nemůže obnovit sadu stránek do aktuálního stavu. Kdy a jak vyřadit protokoly archivace, je popsáno v tématu Vyřazení datových sad protokolu archivace.

Pomocí příkazu `/cpf DIS USAGE TYPE(ALL)` můžete zobrazit protokol RBA a pořadové číslo rozsahu protokolu (LRSN), které potřebujete k obnovení sad stránek správce front a struktur skupiny sdílení front. Poté byste měli použít obslužný program print log map utility (CSQJU004) k tisku informací o datové sadě zaváděcího programu (BSDS) pro správce front k vyhledání protokolů obsahujících protokol RBA.

V případě struktur prostředku CF je třeba spustit obslužný program CSQJU004 pro každého správce front ve skupině sdílení front a vyhledat protokoly obsahující název LRSN. Tyto protokoly a všechny pozdější protokoly potřebujete, abyste mohli obnovit sady stránek a struktury.

Neměnit DDname na přidružení sady stránek

Produkt IBM MQ přidruží sadu stránek číslo 00 s názvem DDname CSQP0000, sadu stránek číslo 01 s názvem DDname CSQP0001atd. až do výše CSQP0099. Produkt IBM MQ zapisuje záznamy protokolu pro zotavení pro sadu stránek na základě názvu DDname, ke kterému je sada stránek přidružena. Z tohoto důvodu nesmíte přesouvat sady stránek, které již byly přidruženy k názvu DDname PSID.

z/OS Obnova sad stránek

Toto téma slouží k pochopení faktorů, které se podílejí na obnově sad stránek, a k minimalizaci doby restartování.

Klíčový faktor ve strategii zotavení se týká doby, po kterou můžete tolerovat výpadek správce front. Celková doba výpadku může zahrnovat dobu potřebnou k obnovení sady stránek ze zálohy nebo k restartování správce front po nestandardním ukončení. Faktory ovlivňující čas restartu zahrnují, jak často zálohujete sady stránek a kolik dat se zapisuje do protokolu mezi kontrolními body.

Chcete-li minimalizovat dobu restartování po nestandardním ukončení, ponechte jednotky práce krátké, aby se při restartování systému používaly maximálně dva aktivní protokoly. Pokud například navrhujete aplikaci IBM MQ , vyhněte se volání MQGET , které má dlouhý interval čekání mezi prvním voláním MQI in-syncpoint a bodem potvrzení, protože to může vést k transakci s dlouhou dobou trvání. Další častou příčinou dlouhých pracovních jednotek jsou intervaly dávek delší než 5 minut pro inicializátor kanálu.

Pomocí příkazu DISPLAY THREAD můžete zobrazit RBA pracovních jednotek a pomoci vyřešit ty staré.

Jak často musíte zálohovat sadu stránek?

Častá záloha sady stránek je nezbytná, pokud je požadována přiměřeně krátká doba obnovy. To platí i v případě, že je sada stránek velmi malá nebo ve frontách v této sadě stránek existuje malé množství aktivity.

Používáte-li trvalé zprávy v sadě stránek, frekvence zálohování by měla být v hodinách, nikoli ve dnech. Toto je také případ pro sadu stránek nula.

Chcete-li vypočítat přibližnou frekvenci zálohování, začněte určením cílové celkové doby obnovy. Skládá se z následujících položek:

1. Doba potřebná k reakci na problém.
2. Doba potřebná k obnovení záložní kopie sady stránek.

   Používáte-li funkci SnapShot pro zálohování/obnovu, doba potřebná k provedení této úlohy je několik sekund. Informace o SnapShotnaleznete v příručce *DFSMSdss Storage Administration Guide*.
3. Čas, který správce front vyžaduje k restartování, včetně času potřebného k obnovení sady stránek.

   To nejvíce závisí na množství dat protokolu, která musí být přečtena z aktivních a archivních protokolů od doby, kdy byla tato sada stránek naposledy zálohována. Všechna taková data protokolu musí být přečtena, kromě těch, která jsou přímo spojena s poškozenou sadou stránek.

   Poznámka: Při použití *fuzzy zálohy* (kde je pořízen snímek protokolů a sad stránek, zatímco je aktivní jednotka práce) může být nutné číst až tři další kontrolní body, což může vést k nutnosti číst jeden nebo více dalších protokolů.

Při rozhodování o tom, jak dlouho povolit obnovu sady stránek, jsou faktory, které je třeba zvážit, následující:

- Rychlost, jakou jsou data zapisována do aktivních protokolů během normálního zpracování, závisí na tom, jak zprávy dorazí do vašeho systému, kromě rychlosti zpráv.

  Zprávy přijaté nebo odeslané prostřednictvím kanálu mají za následek více protokolování dat než zprávy generované a načtené lokálně.
- Rychlost, jakou lze číst data z archivu a aktivních protokolů.

  Při čtení protokolů závisí dosažitelná rychlost přenosu dat na použitých zařízeních a celkovém zatížení konkrétního subsystému DASD.

  U většiny páskových jednotek je možné dosáhnout vyšší rychlosti přenosu dat pro archivované protokoly s velkou velikostí bloku. Pokud je však pro zotavení vyžadován protokol archivace, musí být také přečtena všechna data v aktivních protokolech.

z/OS Obnova struktur prostředku CF

V tomto tématu jsou uvedeny informace o procesu zotavení pro struktury prostředku CF.

Ke zpracování příkazu RECOVER CFSTRUCT musí být aktivní alespoň jeden správce front ve skupině sdílení front. Zotavení struktury prostředku CF nemá vliv na dobu restartování správce front, protože zotavení provádí již aktivní správce front.

Proces obnovy se skládá ze dvou logických kroků, které jsou spravovány příkazem RECOVER CFSTRUCT:

1. Vyhledání a obnova zálohy.
2. Sloučení všech protokolovaných aktualizací trvalých zpráv, které jsou uloženy ve struktuře prostředku CF, z protokolů všech správců front ve skupině sdílení front, kteří používají strukturu prostředku CF, a použití změn na zálohu.

Druhý krok bude pravděpodobně trvat mnohem déle, protože může být nutné číst velké množství dat protokolu. Můžete zkrátit dobu potřebnou k provedení častých záloh nebo k obnovení více struktur prostředku CF současně, případně obojí.

Správce front provádějící zotavení vyhledá příslušné zálohy ve všech protokolech ostatních správců front s použitím dat v souboru Db2 a datových sadách samozavedení. Správce front přehraje tyto zálohy ve správném časovém pořadí v rámci skupiny sdílení front, od těsně před poslední zálohou až po bod selhání.

Doba zotavení struktury prostředku CF závisí na množství dat protokolu pro zotavení, která je třeba přehrát, což závisí na frekvenci zálohování. V nejhorším případě je čtení protokolu správce front stejně dlouhé jako jeho zápis. Máte-li například skupinu sdílení front obsahující šest správců front, může přehrávání aktivity protokolu za hodinu trvat šest hodin. Obecně to trvá kratší dobu, než je tato hodnota, protože čtení lze provádět hromadně a protože protokoly různých správců front lze číst paralelně. Jako výchozí bod doporučujeme zálohovat své struktury CF každou hodinu.

Všichni správci front mohou pokračovat v práci s nesdílenými frontami a frontami v jiných strukturách prostředku CF, pokud existuje neúspěšná struktura prostředku CF. Pokud se také nezdařila administrativní struktura, musí být před zadáním příkazu RECOVER CFSTRUCT spuštěn alespoň jeden ze správců front ve skupině sdílení front.

Zálohování struktur prostředku CF může vyžadovat značnou kapacitu pro zápis do protokolu, a proto může správce front provádějící zálohování zatížit velkou zátěží. Vyberte lehce načteného správce front pro provádění záloh. Pro vytížené systémy přidejte dalšího správce front do skupiny sdílení front a vyhradit jej výhradně pro provádění záloh.

z/OS Dosažení specifických cílů obnovy

V tomto tématu naleznete informace o tom, jak lze dosáhnout specifických cílových časů obnovy přizpůsobením frekvence zálohování.

Máte-li specifické cíle zotavení, které mají dosáhnout například dokončení zpracování obnovy správce front a restartování kromě normálního času spuštění během *xx* sekund, můžete pomocí následujícího výpočtu odhadnout frekvenci zálohování (v hodinách):

```
Formula (A)
                    Required restart time * System recovery log read rate
                         (in secs)                    (in MB/sec)
Backup frequency  = ------------------------------------------------------
   (in hours)              Application log write rate (in MB/hour)
```

Poznámka: Následující příklady jsou určeny ke zvýraznění potřeby často zálohovat sady stránek. Výpočty předpokládají, že většina aktivity protokolu je odvozena z velkého počtu trvalých zpráv. Existují však situace, kdy se množství protokolované aktivity nepočítá snadno. Například v prostředí skupiny sdílení front může jednotka práce, ve které jsou kromě jiných prostředků aktualizovány sdílené fronty, vést

k zápisu záznamů UOW do protokolu IBM MQ . Z tohoto důvodu lze rychlost zápisu do protokolu aplikace ve vzorci (A) přesně odvodit pouze z pozorované rychlosti, kterou protokoly IBM MQ vyplňují.

Zvažte například systém, ve kterém produkt IBM MQ MQI clients vygeneruje celkovou zátěž 100 trvalých zpráv za sekundu. V tomto případě jsou všechny zprávy generovány lokálně.

Pokud má každá zpráva délku uživatele 1 kB, množství dat zaprotokolovaných každou hodinu je přibližně:

```
100 * (1 + 1.3) KB * 3600 = approximately 800 MB

where
      100           = the message rate a second
      (1 + 1.3) KB  = the amount of data logged for
                      each 1 KB of persistent messages
```

Zvažte celkovou cílovou dobu obnovy 75 minut. Pokud jste povolili 15 minut reagovat na problém a obnovit záložní kopii sady stránek, musí být obnova a restart správce front dokončeny do 60 minut (3600 sekund) s použitím vzorce (A). Za předpokladu, že všechna požadovaná data protokolu jsou na serveru RVA2-T82 DASD, který má rychlost obnovy přibližně 2.7 MB za sekundu, je nutné, aby frekvence zálohování sady stránek byla alespoň jednou za:

```
3600 seconds * 2.7 MB a second / 800 MB an hour = 12.15 hours
```

Pokud váš den aplikace IBM MQ trvá přibližně 12 hodin, je vhodná jedna záloha každý den. Pokud však den aplikace trvá 24 hodin, jsou vhodnější dvě zálohy každý den.

Dalším příkladem může být produkční systém, ve kterém jsou všechny zprávy určeny pro aplikace typu požadavek-odezva (tj. trvalá zpráva je přijímána přijímacím kanálem a trvalá zpráva odpovědi je generována a odeslána odesílacím kanálem).

V tomto příkladu je dosažená velikost dávky jedna, a proto existuje jedna dávka pro každou zprávu. Pokud existuje 50 odpovědí na požadavek za sekundu, celkové načtení je 100 trvalých zpráv za sekundu. Je-li každá zpráva dlouhá 1 kB, množství dat zaprotokolovaných každou hodinu je přibližně:

```
50((2 * (1+1.3) KB) + 1.4 KB + 2.5 KB) * 3600 = approximately 1500 MB

where:
 50                 = the message pair rate a second
 (2 * (1 + 1.3) KB) = the amount of data logged for each message pair
 1.4 KB             = the overhead for each batch of messages
                      received by each channel
 2.5 KB             = the overhead for each batch of messages sent
                      by each channel
```

Chcete-li dosáhnout zotavení a restartování správce front během 30 minut (1800 sekund) a znovu předpokládat, že všechna požadovaná data protokolu jsou na RVA2-T82 DASD, je nutné, aby se zálohování sady stránek provádělo alespoň jednou za:

```
1800 seconds * 2.7 MB a second / 1500 MB an hour = 3.24 hours
```

Pravidelná kontrola frekvence zálohování

Monitorujte využití protokolu IBM MQ v MB za hodinu. Pravidelně provádějte tuto kontrolu a v případě potřeby změňte frekvenci zálohování sady stránek.

z/OS Pokyny k zálohování pro ostatní produkty

Pokud používáte produkt IBM MQ s produktem CICS nebo IMS , musíte také zvážit důsledky pro vaši strategii zálohování s těmito produkty. Správce datových úložišť DFHSM (Data Facility Hierarchical Storage Manager) spravuje datové úložiště a může interaktivně spolupracovat s úložištěm používaným produktem IBM MQ.

Zálohování a obnova pomocí DFHSM

Správce datových úložišť DFHSM (Data Facility Hierarchical Storage Manager) provádí automatickou správu dostupnosti prostoru a dostupnosti dat mezi úložnými zařízeními ve vašem systému. Pokud jej použijete, musíte vědět, že přesouvá data do a z úložiště IBM MQ automaticky.

DFHSM efektivně spravuje prostor DASD přesunutím datových sad, které nebyly v poslední době použity k alternativnímu úložišti. Také zpřístupňuje data pro obnovu automatickým kopírováním nových nebo změněných datových sad na pásky nebo záložní nosiče DASD. Může odstranit datové sady nebo je přesunout na jiné zařízení. Jeho operace se provádějí denně, v určený čas, a umožňují uchovávat datovou sadu po předem stanovenou dobu před jejím odstraněním nebo přesunutím.

Můžete také provést všechny operace DFHSM ručně. Další informace o DFHSM naleznete v dokumentaci k produktu z/OS DFSMS . Pokud používáte DFHSM s IBM MQ, všimněte si, že DFHSM provádí následující:

- Používá katalogizované datové sady.
- Pracuje se sadami stránek a protokoly.
- Podporuje datové sady VSAM.

Obnova a CICS

Obnova prostředků CICS není ovlivněna přítomností IBM MQ. Produkt CICS rozpoznává IBM MQ jako jiný prostředek nežCICS (nebo externí správce prostředků) a zahrnuje produkt IBM MQ jako účastníka všech požadavků na koordinaci synchronizačních bodů pomocí rozhraní RMI (CICS resource manager interface). Další informace o obnově systému CICS a rozhraní správce prostředků systému CICS naleznete v dokumentaci k produktu CICS .

Obnova a IMS

IMS rozpoznává IBM MQ jako externí subsystém a jako účastníka v koordinaci synchronizačních bodů. IMS zotavení pro externí prostředky subsystému je popsáno v dokumentaci k produktu IMS .

z/OS Příprava na obnovu na alternativním serveru

Pokud dojde k celkové ztrátě výpočetního centra IBM MQ , můžete provést obnovu na jiném systému IBM MQ na serveru pro obnovu.

Chcete-li obnovit systém IBM MQ na serveru pro obnovu, musíte pravidelně zálohovat sady stránek a protokoly. Stejně jako u všech operací obnovy dat je cílem zotavení z havárie ztratit co nejméně dat, zpracování pracovní zátěže (aktualizace) a čas, jak je to možné.

Na místě obnovy:

- Zotavení IBM MQ správce front **musí** mít stejný název jako ztracený správce front.
- Ujistěte se, že modul systémových parametrů použitý ve správci front pro zotavení obsahuje stejné parametry jako ztracený správce front.

Další informace viz Administrace IBM MQ for z/OS a Odstraňování problémů IBM MQ for z/OS .

z/OS Příklad aktivity zálohování správce front

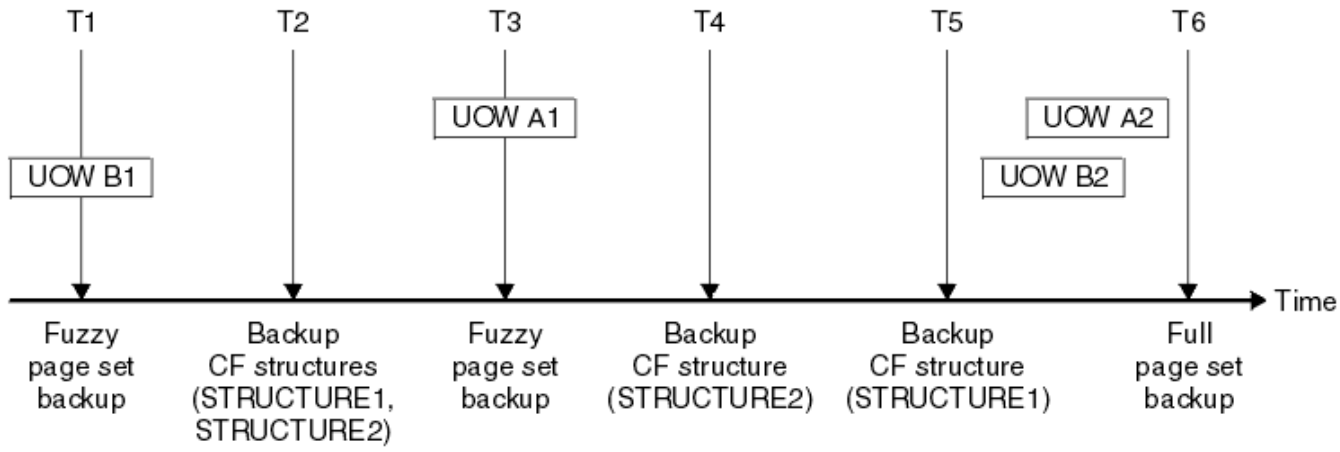
Toto téma se zobrazuje jako příklad aktivity zálohování správce front.

Při plánování strategie zálohování správce front je klíčovým aspektem uchování správného množství dat protokolu. Správa protokolů popisuje, jak určit, které datové sady protokolu jsou vyžadovány, s odkazem na adaptér RBA pro zotavení systému správce front. IBM MQ určuje RBA obnovy systému pomocí následujících informací:

- Momentálně aktivní jednotky práce.
- Aktualizace sad stránek, které dosud nebyly vyprázdněny z fondů vyrovnávacích pamětí na disk.
- Zálohy struktury prostředku CF a informace o tom, zda protokol tohoto správce front obsahuje informace nezbytné pro všechny operace zotavení, které je používají.

Musíte uchovat dostatek dat protokolu, abyste mohli provést obnovu médií. Zatímco se RBA obnovy systému v průběhu času zvyšuje, množství dat protokolu, která musí být uchována, se při provádění následných záloh sníží. Zálohy struktury prostředku CF jsou spravovány produktem IBM MQ, a proto jsou brány v úvahu při vytváření sestav RBA obnovy systému. To znamená, že v praxi se množství dat protokolu, která musí být uchována, sníží pouze při vytváření záloh sad stránek.

V části Obrázek 43 na stránce 193 je uveden příklad aktivity zálohování ve správci front, který je členem skupiny sdílení front, způsob, jakým se adaptér RBA pro zotavení liší podle jednotlivých záloh a jaký vliv má na množství dat protokolu, která je třeba zachovat. V tomto příkladu používá správce front lokální a sdílené prostředky: sady stránek a dvě struktury prostředku CF, STRUCTURE1 a STRUCTURE2.



Obrázek 43. Příklad aktivity zálohování správce front

To je to, co se děje v každém okamžiku:

Časový bod T1

Z vašich sad stránek se vytvoří fuzzy záloha, jak je popsáno v tématu Jak zálohovat a obnovit sady stránek.

Adresa RBA zotavení systému správce front je nejnižší z následujících hodnot:

- Nápravné sady RBA sad stránek, které se v tomto bodě zálohují.
- Nejnižší adresa RBA zotavení požadovaná pro zotavení struktur aplikace prostředku CF. To souvisí s obnovou záloh struktury STRUCTURE1 a STRUCTURE2 vytvořených dříve.
- Adresa RBA zotavení pro nejstarší aktuálně aktivní transakci v rámci správce front (UOWB1).

Adaptér RBA obnovy systému pro tento časový bod je dán zprávami vydanými příkazem DISPLAY USAGE, který je součástí procesu fuzzy zálohy.

Časový bod T2

Vytvoří se zálohy struktur prostředku CF. Nejprve je zálohována struktura prostředku CF STRUCTURE1 a poté STRUCTURE2.

Množství dat protokolu, která musí být zachována, se nezměnilo, protože stejná data, která jsou určena z adaptéru RBA pro zotavení systému na adrese T1 , jsou stále vyžadována pro obnovu pomocí záloh sady stránek vytvořených na T1.

Časový okamžik T3
Vytvoří se další fuzzy záloha.

Adresa RBA zotavení systému správce front je nejnižší z následujících hodnot:

- Nápravné sady RBA sad stránek, které se v tomto bodě zálohují.
- Nejnižší hodnota zotavení RBA vyžadovaná pro obnovení struktury prostředku Coupling Facility STRUCTURE1, protože příkaz STRUCTURE1 byl zálohován před příkazem STRUCTURE2.
- Adresa RBA zotavení pro nejstarší aktuálně aktivní jednotku práce v rámci správce front (UOWA1).

Adaptér RBA obnovy systému pro tento časový bod je dán zprávami vydanými příkazem DISPLAY USAGE, který je součástí procesu fuzzy zálohy.

Nyní můžete omezit uchovaná data protokolu, jak je určeno tímto novým adaptérem RBA pro obnovu systému.

Časový bod T4
Provede se záloha struktury prostředku CF STRUCTURE2. Adresa RBA zotavení pro obnovu nejstarší požadované zálohy struktury prostředku CF se vztahuje k záloze struktury prostředku CF STRUCTURE1, která byla zálohována v čase T2.

Vytvoření této zálohy struktury prostředku CF nemá žádný vliv na množství dat protokolu, která musí být zachována.

Časový okamžik T5
Je vytvořena záloha struktury prostředku CF STRUCTURE1. Adresa RBA pro obnovení nejstarší požadované zálohy struktury prostředku CF nyní souvisí s obnovou struktury prostředku CF STRUCTURE2, která byla zálohována v čase T4.

Vytvoření této zálohy struktury prostředku CF nemá žádný vliv na množství dat protokolu, která musí být zachována.

Časový okamžik T6
Ze sad stránek se provede úplná záloha, jak je popsáno v tématu Jak zálohovat a obnovit sady stránek.

Adresa RBA zotavení systému správce front je nejnižší z následujících hodnot:

- Nápravné sady RBA sad stránek, které se v tomto bodě zálohují.
- Nejnižší zotavení RBA požadované pro obnovení struktur prostředku CF. To souvisí s obnovením struktury prostředku CF STRUCTURE2.
- Adresa RBA zotavení pro nejstarší aktuálně aktivní jednotku práce v rámci správce front. V tomto případě neexistují žádné aktuální jednotky práce.

Adresa RBA obnovy systému pro tento časový bod je dána zprávami vydanými příkazem DISPLAY USAGE, který je součástí procesu úplné zálohy.

Uchovaná data protokolu lze opět snížit, protože obnova systému RBA přidružená k úplné záloze je novější.

z/OS Plánování prostředí z/OS UNIX

Určité procesy v rámci správce front IBM MQ , inicializátoru kanálu a serveru mqweb používají pro své normální zpracování funkci z/OS UNIX System Services (z/OS UNIX).

ID uživatelů spuštěných úloh správce front a inicializátoru kanálu vyžadují segment OMVS s definovaným UID, aby bylo možné přistupovat k produktu z/OS UNIX. ID uživatelů nevyžadují v produktu z/OS UNIXžádná speciální oprávnění.

Poznámka: Ačkoli správce front a inicializátor kanálu využívají mechanizmy produktu z/OS UNIX (například pro rozhraní se službami TCP/IP), nemusí přistupovat k žádnému obsahu instalačního adresáře produktu IBM MQ v systému souborů z/OS UNIX . V důsledku toho správce front a inicializátor kanálu nevyžadují žádnou konfiguraci k určení cesty pro systém souborů z/OS UNIX .

Server mqweb, který je hostitelem serverů IBM MQ Console a REST API, používá soubory v instalačním adresáři IBM MQ v systému souborů z/OS UNIX . Také potřebuje přístup k jinému systému souborů, který se používá k ukládání dat, jako jsou konfigurační soubory a soubory protokolu. Soubor JCL spuštěné úlohy mqweb je třeba upravit tak, aby odkazoval na tyto systémy souborů z/OS UNIX .

Obsah adresáře IBM MQ v systému souborů z/OS UNIX používají také aplikace, které se připojují k produktu IBM MQ. Například aplikace používající rozhraní IBM MQ classes for Java nebo IBM MQ classes for JMS .

Příslušné pokyny ke konfiguraci naleznete v následujících tématech:

- Proměnné prostředí relevantní pro IBM MQ classes for Java
- IBM MQ classes for Java knihovny
- Nastavení proměnných prostředí
- Konfigurace knihoven Java Nativní rozhraní (JNI)

z/OS Plánování pro Advanced Message Security

TLS (nebo SSL) lze použít k šifrování a ochraně zpráv proudících v síti, ale to neochrání zprávy, když jsou ve frontě ("v klidu"). Advanced Message Security (AMS) chrání zprávy před jejich prvním vložením do fronty, dokud nejsou přijaty, aby je mohli číst pouze zamýšlení příjemci zprávy. Zprávy jsou šifrovány a podepsány během zpracování vložení a nechráněny během zpracování získání.

Produkt AMS lze nakonfigurovat tak, aby chránil zprávy různými způsoby:

1. Zpráva může být podepsána. Zpráva je v čistém textu, ale existuje kontrolní součet, který je podepsán. To umožňuje zjištění jakýchkoli změn v obsahu zprávy. Z podepsaného obsahu můžete identifikovat, kdo podepsal data.
2. Zpráva může být zašifrována. Obsah není viditelný pro nikoho bez dešifrovacího klíče. Dešifrovací klíč je šifrován pro každého příjemce.
3. Zpráva může být zašifrována a podepsána. Dešifrovací klíč je šifrován pro každého příjemce a z podpisu můžete identifikovat, kdo zprávu odeslal.

Šifrování a podepisování používá digitální certifikáty a svazky klíčů.

Klienta můžete nastavit tak, aby používal produkt AMS, takže data budou chráněna před vložením dat do kanálu klienta. Chráněné zprávy lze odeslat vzdálenému správci front a je třeba konfigurovat vzdáleného správce front pro zpracování těchto zpráv.

nastaveníAMS

Pro práci s produktem AMS se používá adresní prostor AMS . To má další nastavení zabezpečení, které umožní přístup a ochranu používání kroužků klíčů a certifikátů.

Můžete nakonfigurovat, které fronty mají být chráněny, pomocí obslužného programu (CSQ0UTIL), který definuje zásady zabezpečení pro fronty.

Po nastavení produktu AMS

Musíte nastavit digitální certifikát a svazek klíčů pro lidi, kteří vkládají zprávy, a pro osoby, které zprávy dostávají.

Pokud uživatel Alice v systému z/OS potřebuje odeslat zprávu Bobovi, AMS potřebuje kopii veřejného certifikátu pro Boba.

Pokud chce Bob zpracovat zprávu od Alice, produkt AMS potřebuje veřejný certifikát pro Alice nebo stejný certifikát certifikační autority, který Alice používá.

Upozornění: Musíte provést následující akce:

- Pečlivě naplánujte, kdo může vkládat do front nebo se z nich dostat.
- Identifikujte osoby a jejich názvy certifikátů.

Je snadné dělat chyby a problémy mohou být těžké vyřešit.

Související pojmy

“Plánování pro vašeho správce front” na stránce 141

Při nastavování správce front by vaše plánování mělo umožnit růst správce front tak, aby splňoval potřeby vašeho podniku.

z/OS Plánování pro Managed File Transfer

Tento oddíl slouží jako vodítko pro nastavení systému pro spuštění Managed File Transfer (MFT) na systému z/OS.

z/OS Plánování pro Managed File Transfer -hardwarové a softwarové požadavky

Toto téma použijte jako vodítko pro nastavení hardwarových a softwarových požadavků na vašem systému, abyste spustili Managed File Transfer (MFT) na systému z/OS.

Softwarové požadavky

Managed File Transfer je napsáno v souboru Java, s některými skripty shellu a JCL pro konfiguraci a provoz programu.

Důležité: Musíte být obeznámeni s z/OS UNIX System Services (z/OS UNIX), abyste mohli konfigurovat Managed File Transfer. Příklad:

- Adresářová struktura souboru s názvy, jako např. `/u/userID/myfile.txt`
- Příkazy systému z/OS UNIX , například:
  - `cd` (změnit adresář)
  - `ls` (seznam)
  - `chmod` (změna oprávnění k souboru)
  - `chown` (změnit vlastnictví souboru nebo skupiny, které mají přístup k souboru nebo adresáři)

Chcete-li mít možnost konfigurovat a spouštět MFT, musíte mít v produktu z/OS UNIX následující produkty:

1. Java, například v adresáři `/java/java80_bit64_GA/J8.0_64/`
2. IBM MQ 9.3.0, například v adresáři `/mqm/V9R3M0`
3. Chcete-li použít produkt Db2 pro stav a historii, musíte nainstalovat knihovny Db2 JDBC , například v adresáři `/db2/db2v10/jdbc/libs`.

Registrace produktu

Při spuštění Managed File Transfer zkontroluje registraci ve zřetězení `sys1.parmlib`(IFAPRDxx). Následující kód je příkladem registrace MFT:

```
PRODUCT OWNER('IBM CORP')
NAME('WS MQ FILE TRANS')
ID(5655-MFT)
VERSION(*) RELEASE(*) MOD(*)
```

```
FEATURENAME('WS MQ FILE TRANS')
STATE(ENABLED)
```

Prostor na disku

Adresář IBM MQ for z/OS Program Directory uvádí požadavky na úložiště DASD a zFS pro Managed File Transfer. Odkazy ke stažení adresáře programu pro systém IBM MQ for z/OSnaleznete v části IBM MQ 9.3 Soubory PDF pro dokumentaci k produktu a Adresáře programů.

z/OS Plánování pro Managed File Transfer -topologie

Toto téma použijte jako vodítko pro topologii, kterou potřebujete ve svém systému ke spuštění Managed File Transfer (MFT) na systému z/OS.

Managed File Transfer Správci front

IBM MQ Managed File Transfer topologie se skládají z:

Agenti a jejich přidružení správci front
Agent používá systémové fronty, jejichž hostitelem je správce front agenta, aby udržoval informace o stavu a přijímal požadavky na práci.

Správce front příkazů
Jedná se o bránu do topologie produktu MFT . Je připojen ke správcům front agenta prostřednictvím odesílacích a přijímacích kanálů nebo klastrování. Jsou-li spuštěny určité příkazy, připojí se přímo ke správci front příkazů a odešlou zprávu určenému agentu. Tato zpráva je směrována prostřednictvím sítě IBM MQ do správce front agenta, kde je vyzvednuta agentem a zpracována.

Koordinační správce front
Jedná se o centrální rozbočovač, který má znalosti o celé topologii. Koordinační správce front je připojen ke všem správcům front agenta v topologii prostřednictvím odesílacího a přijímacího kanálu nebo pomocí klastrování. Agenti pravidelně publikují informace o stavu do koordinačního správce front a ukládají tam své šablony přenosu.

Jeden správce front může v rámci topologie provádět více rolí. Například stejného správce front lze konfigurovat jako koordinačního správce front i správce front příkazů pro topologii.

Pokud používáte více správců front, musíte nastavit kanály mezi správci front. To můžete provést buď pomocí klastrování, nebo pomocí dvoubodových připojení.

Při použití produktu IBM MQ Managed File Transfer for z/OSje třeba při určování správců front, kteří mají být použiti pro různé role v rámci topologie, zvážit několik věcí.

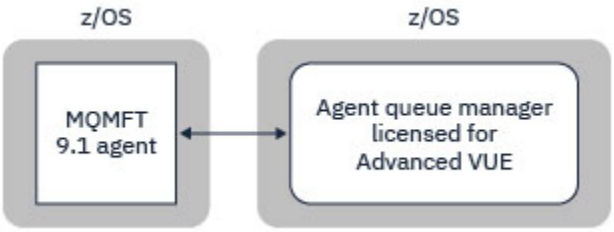
Správci front agenta

Správce front agenta pro agenta IBM MQ Managed File Transfer for z/OS musí být spuštěn v systému z/OS.

Pokud:

- Agent spouští Managed File Transfer for z/OS na systému IBM MQ 9.1 nebo novějším
- A správce front agenta je licencován pro produkt IBM MQ Advanced for z/OS Value Unit Edition (Advanced VUE)

agent se může připojit ke správci front pomocí přenosu CLIENT.



Obrázek 44. MFT 9.1 agenti v systému z/OS se mohou připojit ke správci front pomocí přenosu CLIENT za předpokladu, že je správce front licencován pro produkt Advanced VUE.

Pokud:

- Agent spouští Managed File Transfer for z/OS na systému IBM MQ 9.0 nebo starším
- Nebo je správce front agenta spuštěn Managed File Transfer for z/OS v systému IBM MQ 9.0 nebo novějším a správce front agenta je licencován buď pro MFT, IBM MQ Advanced for z/OS, nebo Advanced VUE .

agent se musí připojit ke správci front pomocí přenosu BINDINGS.

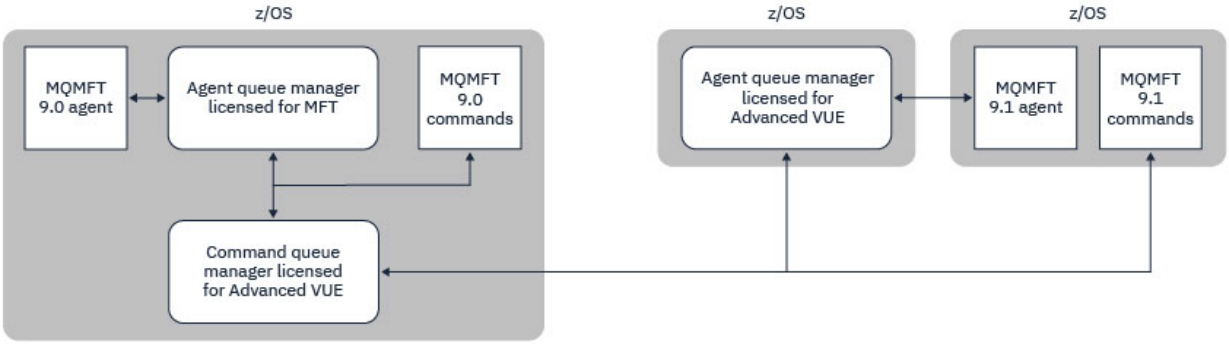
Obrázek 45. Agenti MFT 9.0 na agentech z/OS a 9.1 , kteří mají licencovaného správce front agenta pro MFT nebo IBM MQ Advanced, se musí připojit pomocí přenosu BINDINGS.

Správci front příkazů

Téma Které příkazy a procesy systému MFT se připojují ke kterému správci front zobrazuje všechny příkazy, které se připojují ke správci front příkazů pro topologii Managed File Transfer .

Poznámka: Při spouštění těchto příkazů v systému z/OSmusí být správce front příkazů také v systému z/OS.

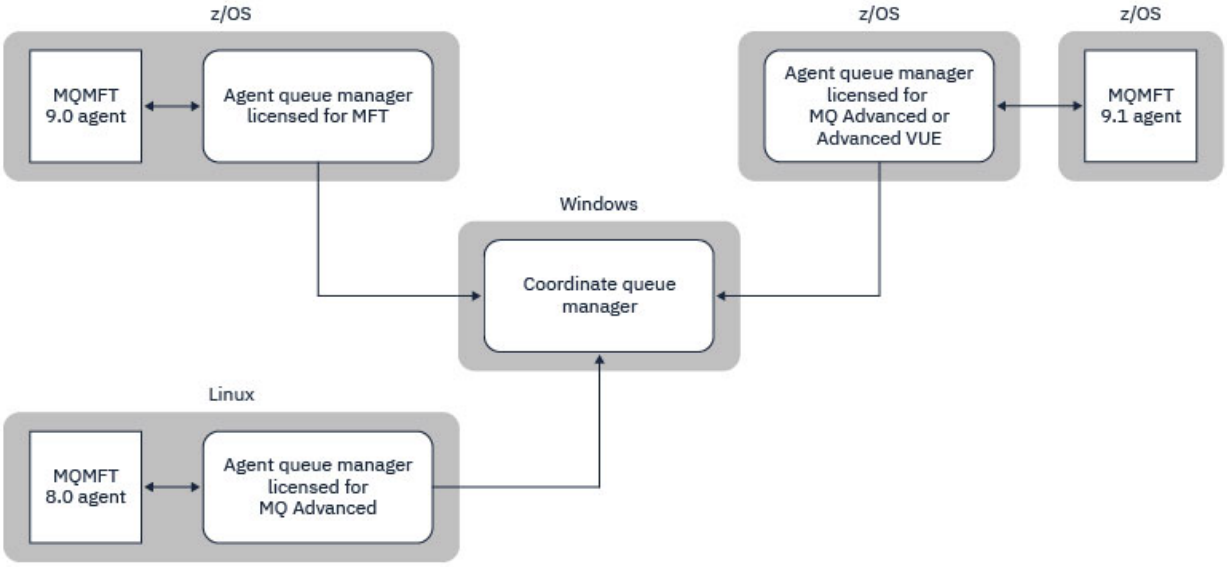
Pokud je správce front příkazů licencován pro produkt Advanced VUE, mohou se příkazy připojit ke správci front pomocí přenosu CLIENT. Jinak se musí příkazy připojit ke správci front příkazů pomocí přenosu BINDINGS.



Obrázek 46. Příkazy se připojují ke správci front příkazů pro topologii MFT. Při spouštění těchto příkazů v systému z/OSmusí být správce front příkazů také v systému z/OS .

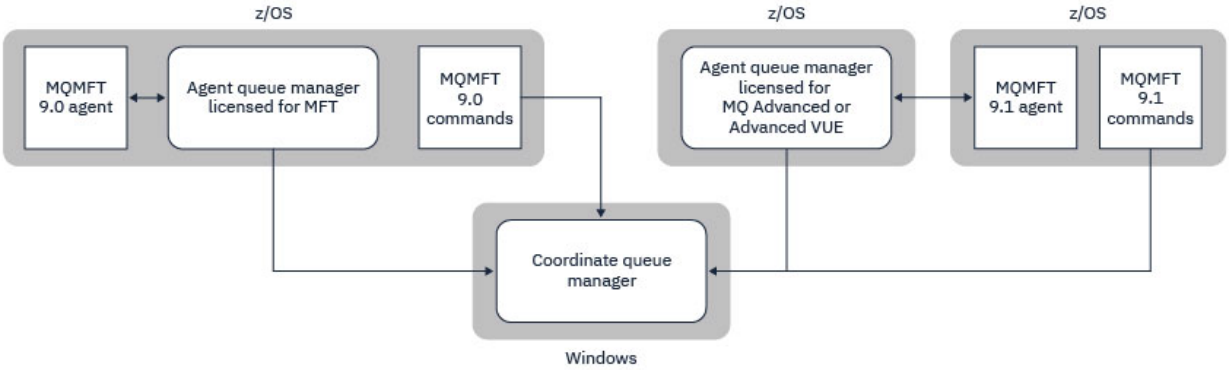
Koordinační správci front

Agenti produktu IBM MQ Managed File Transfer for z/OS mohou být součástí topologie, v níž je koordinační správce front spuštěn v systému z/OS, nebo v prostředí s více platformami.



Obrázek 47. Agenti MFT běžící v systému z/OS mohou být součástí topologie MFT, kde je koordinační správce front spuštěn na multiplatformě IBM MQ .

Téma Které MFT příkazy a procesy se připojují ke kterému správci front zobrazuje příkazy, které se připojují ke koordinačnímu správci front pro topologii produktu Managed File Transfer . Tyto příkazy lze spustit v systému z/OS a poté se připojit ke koordinačnímu správci front spuštěnému na jiné platformě.



*Obrázek 48. Určité příkazy, například **fteListAgents**, se připojují přímo ke koordinačnímu správci front pro topologii produktu MFT .*

Kolik agentů potřebuji?

Agenti dělají práci při přenosu dat, a když zadáte požadavek na přenos dat, uvedete název agenta.

Standardně může agent souběžně zpracovat 25 požadavků na odeslání a 25 požadavků na příjem. Tyto procesy můžete konfigurovat. Další informace viz Managed File Transfer volby konfigurace na serveru z/OS .

Pokud je agent zaneprázdněn, je práce zařazena do fronty. Doba potřebná ke zpracování požadavku závisí na více faktorech, například na množství dat, která mají být odeslána, na šířce pásma sítě a na prodlevě v síti.

Možná budete chtít mít více agentů pro paralelní zpracování.

Můžete také řídit, ke kterým prostředkům má agent přístup, takže můžete chtít, aby někteří agenti pracovali s omezenou podmnožinou dat.

Chcete-li zpracovat požadavky s jinou prioritou, můžete použít více agentů a použít správce pracovní zátěže k nastavení priority úloh.

Spuštění agentů

Agenti jsou obvykle procesy s dlouhou dobou zpracování. Procesy lze zadat jako úlohy, které se spouštějí v dávkovém zpracování, nebo jako spuštěné úlohy.

z/OS Plánování pro Managed File Transfer -aspekty zabezpečení

Toto téma použijte jako vodítko k tomu, jaké aspekty zabezpečení potřebujete ve svém systému ke spuštění Managed File Transfer (MFT) na systému z/OS.

Zabezpečení

Musíte identifikovat, která ID uživatelů budou použita pro konfiguraci MFT a pro operaci MFT.

Musíte identifikovat soubory nebo fronty, které přenášíte, a která ID uživatelů budou zadávat požadavky na přenos do MFT.

Když upravíte agenty a modul protokolování, uvedete skupinu uživatelů, kteří mohou spouštět služby MFT, nebo provedete administraci MFT.

Tuto skupinu byste měli nastavit před tím, než začnete upravovat MFT. Vzhledem k tomu, že MFT používá fronty IBM MQ , pokud máte ve správci front povoleno zabezpečení, vyžaduje MFT přístup k následujícím prostředkům:

Tabulka 26. Třída prostředků MQADMIN

Název	**Vyžadován přístup**
QUEUE.SYSTEM.FTE.EVENT.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.COMMAND.agent_name	Aktualizovat
CONTEXT.SYSTEM.FTE.COMMAND.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.STATE.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.DATA.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.REPLY.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.AUTHAGT1.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.AUTHTRN1.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.AUTHOPS1.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.AUTHSCH1.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.AUTHMON1.agent_name	Aktualizovat
QUEUE.SYSTEM.FTE.AUTHADM1.agent_name	Aktualizovat

Tabulka 27. Třída prostředků MQQUEUE

Název	**Vyžadován přístup**
SYSTEM.FTE.AUTHAGT1.agent_name	Aktualizovat
SYSTEM.FTE.AUTHTRN1.agent_name	Aktualizovat
SYSTEM.FTE.AUTHOPS1.agent_name	Aktualizovat
SYSTEM.FTE.AUTHSCH1.agent_name	Aktualizovat

Tabulka 27. Třída prostředků MQQUEUE (pokračování)	
Název	**Vyžadován přístup**
SYSTEM.FTE.AUTHMON1.agent_name	Aktualizovat

Pomocí pískoviště uživatele můžete určit, ke kterým částem systému souborů má uživatel, který požaduje přenos, přístup.

Chcete-li povolit pískoviště uživatele, přidejte příkaz `userSandboxes=true` do souboru *agent.properties* pro agenta, kterého chcete omezit, a přidejte odpovídající hodnoty do souboru `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/agents/agent_name/UserSandboxes.xml` .

Další informace viz Práce s pískovišti uživatele .

Toto ID uživatele je konfigurováno v souborech `UserSandboxes.xml` .

Tento soubor XML má informace jako ID uživatele nebo ID uživatele * a seznam prostředků, které lze použít (zahrnout) nebo je nelze použít (vyloučit). Musíte definovat specifická ID uživatelů, která mohou přistupovat ke kterým prostředkům: například:

Tabulka 28. Příklad ID uživatele spolu s přístupem ke specifickým prostředkům			
Jméno uživatele	**Přístup**	**Zahrnout nebo vyloučit**	**Prostředek**
Administrátor *	Číst	Zahrnout	`/home/user/**`
Administrátor *	Číst	Vyloučit	`/home/user/private/**`
Sysprog	Číst	Zahrnout	`/home/user/**`
Administrátor *	Číst	Zahrnout	Application.reply.queue

Notes:

1. Pokud je zadána volba `type=queue` , je prostředek buď názvem fronty, nebo názvem fronty `queue@qmgr`.
2. Pokud prostředek začíná řetězcem `//`, jedná se o datovou sadu; jinak se jedná o soubor v adresáři z/OS UNIX.
3. ID uživatele je ID uživatele ze struktury MQMD, takže nemusí odpovídat ID uživatele, který zprávu skutečně vkládá.
4. Pro požadavky v lokálním správci front můžete použít MQADMIN CONTEXT.* abyste omezili, kteří uživatelé mohou tuto hodnotu nastavit.
5. U požadavků přicházejících přes vzdáleného správce front je třeba předpokládat, že distribuovaní správci front mají povoleno zabezpečení, aby se zabránilo neoprávněnému nastavení ID uživatele ve struktuře MQMD.
6. ID uživatele SYSPROG1 na počítači se systémem Linux je stejné ID uživatele SYSPROG1 pro kontrolu zabezpečení systému z/OS.

z/OS Plánování použití IBM MQ Console a REST API na z/OS

IBM MQ Console a REST API jsou aplikace, které běží na serveru WebSphere Liberty (Liberty) známém jako mqweb. Server mqweb je spuštěn jako spuštěná úloha. Produkt IBM MQ Console umožňuje použití webového prohlížeče k administraci správců front. Produkt REST API poskytuje jednoduché programové rozhraní pro aplikace k provádění administrace správců front a k provádění systému zpráv.

Instalační a konfigurační soubory

Musíte nainstalovat funkci IBM MQ for z/OS UNIX System Services Web Components , která nainstaluje soubory potřebné ke spuštění serveru mqweb v produktu z/OS UNIX System Services (z/OS UNIX). Musíte být obeznámeni s produktem z/OS UNIX , abyste mohli konfigurovat a spravovat server mqweb.

Informace o instalaci produktu IBM MQ for z/OS UNIX System Services Componentsnaleznete v tématu IBM MQ for z/OS Soubory PDF adresáře programu .

Soubory IBM MQ v adresáři z/OS UNIX jsou nainstalovány s různými nastavenými atributy, které jsou nezbytné pro správnou činnost serveru mqweb. Potřebujete-li zkopírovat instalační soubory produktu IBM MQ z/OS UNIX , například pokud jste nainstalovali produkt IBM MQ na jeden systém, a spustit produkt IBM MQ na jiném systému, měli byste zkopírovat systém IBM MQ ZFS vytvořený během instalace a připojit jej pouze pro čtení na místo určení. Kopírování souborů jinými způsoby může způsobit ztrátu některých atributů souboru.

Při vytváření serveru mqweb musíte rozhodnout o umístění pro uživatelský adresář Liberty a vytvořit jej. Tento adresář obsahuje konfigurační soubory a soubory protokolu a umístění může být podobné adresáři `/var/mqm/mqweb`.

Použití IBM MQ Console a REST API se správci front na různých úrovních

Produkt REST API může přímo interaktivně spolupracovat pouze se správci front, kteří jsou spuštění ve stejné verzi, vydání a modifikaci (VRM) jako server mqweb, který spouští REST API. Produkt IBM MQ 9.3.0 REST API může například přímo komunikovat pouze s lokálními správci front v adresáři IBM MQ 9.3.0a produkt IBM MQ 9.2.5 REST API může přímo komunikovat pouze s lokálními správci front v adresáři IBM MQ 9.2.5.

Produkt REST API můžete použít k administraci správce front v jiné verzi ze serveru mqweb konfigurací správce front brány. Musíte však mít alespoň jednoho správce front ve stejné verzi jako server mqweb, aby fungoval jako správce front brány. Další informace viz Vzdálená administrace pomocí REST API.

IBM MQ Console lze použít ke správě lokálních správců front, kteří jsou spuštění ve stejné verzi jako IBM MQ Console. V 9.3.0 Od produktu IBM MQ 9.3.0můžete produkt IBM MQ Console také použít k administraci správce front spuštěného ve vzdáleném systému nebo v jiné verzi produktu IBM MQ Console. Další informace naleznete v tématu Přidání vzdáleného správce front do konzoly IBM MQ Console.

Migration

Máte-li pouze jednoho správce front, můžete spustit server mqweb jako jedinou spuštěnou úlohu a změnit knihovny, které používá při migraci správce front.

Máte-li více než jednoho správce front, můžete během migrace spustit servery mqweb v různých verzích pomocí spuštěných úloh s různými názvy. Tato jména mohou být libovolná. Můžete například spustit server IBM MQ 9.1.0 mqweb pomocí spuštěné úlohy s názvem MQWB0910a server IBM MQ 9.0.5 mqweb pomocí spuštěné úlohy s názvem MQWB0905.

Poté při migraci správců front z jedné verze na novější verzi budou tito správci front k dispozici na serveru mqweb pro novější verzi a nebudou již k dispozici na serveru mqweb pro starší verzi.

Po migraci všech správců front na novější verzi můžete odstranit server mqweb pro starší verzi.

Porty HTTP

Server mqweb používá pro HTTPaž dva porty:

- Jedna pro HTTPSs výchozí hodnotou 9443.
- Jedna pro HTTP. Volba HTTP není standardně povolena, ale je-li povolena, má výchozí hodnotu 9080.

Pokud se používají výchozí hodnoty portů, musíte přidělit další porty. Pokud máte více než jeden server mqweb spuštěný současně pro více než jednu verzi produktu IBM MQ, musíte pro každou verzi přidělit

samostatné porty. Další informace o nastavení portů, které používá server mqweb, naleznete v tématu Konfigurace portů HTTP a HTTPS.

K zobrazení informací o portu můžete použít následující příkaz TSO:

```
NETSTAT TCP tcpip (PORT portNumber)
```

kde *tcpip* je název adresního prostoru TCP/IP a *portNumber* uvádí číslo portu, o kterém se mají zobrazit informace.

Zabezpečení-spuštění serveru mqweb

ID uživatele serveru mqweb potřebuje určitá oprávnění. Další informace naleznete v tématu Oprávnění vyžadovaná ID uživatele spuštěné úlohy serveru mqweb.

Zabezpečení-použití IBM MQ Console a REST API

Když použijete IBM MQ Console a REST API, musíte se ověřit jako uživatel, který je zahrnutý v nakonfigurovaném registru. Těmto uživatelům jsou přiřazeny specifické role, které určují akce, které mohou uživatelé provádět. Chcete-li například použít messaging REST API, musí být uživateli přiřazena role `MQWebUser` . Další informace o dostupných rolích pro IBM MQ Console a REST APIa o přístupu, který tyto role udělují, viz téma Role na IBM MQ Console a REST API.

Další informace o konfiguraci zabezpečení pro IBM MQ Console a REST APInaleznete v části IBM MQ Console a REST API zabezpečení.

Poznámky

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

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

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

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

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

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

Následující odstavec se netýká Spojeného království ani jiných zemí, ve kterých je takovéto vyjádření v rozporu s místními zákony: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE "TAK, JAK JE" BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás toto omezení nemusí vztahovat.

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

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

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

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

IBM Corporation
Koordinátor interoperability softwaru, oddělení 49XA
3605 Dálnice 52 N

Rochester, MN 55901
U.S.A.

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

Licencovaný program popsaný v těchto informacích a veškerý licencovaný materiál, který je pro něj k dispozici, jsou poskytovány společností IBM na základě podmínek IBM Smlouvy se zákazníkem, IBM Mezinárodní licenční smlouvy pro programy nebo jiné ekvivalentní smlouvy mezi námi.

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

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

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

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

LICENČNÍ INFORMACE:

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

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

Informace o programovacím rozhraní

Informace o programovacím rozhraní, jsou-li poskytnuty, jsou určeny k tomu, aby vám pomohly vytvořit aplikační software pro použití s tímto programem.

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

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

Důležité: Tyto informace o diagnostice, úpravách a ladění nepoužívejte jako programovací rozhraní, protože se mohou měnit.

Ochranné známky

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

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

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

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

Tento produkt zahrnuje software vyvinutý projektem Eclipse (https://www.eclipse.org/).

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

Číslo položky:

(1P) P/N: