9.2

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 k verzi 9 vydání 2 produktu IBM® MQ a ke všem následujícím vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak.

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

Obsah

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 produktu IBM MQ se seznamte se základními koncepty produktu IBM MQ . Viz IBM MQ Technical overview.

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 vašich distribuovaných front a klastrů” na stránce 19
  - “Plánování distribuované sítě pro publikování/odběr” na stránce 70

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:

- Verze LTS (Long Term Support) je nejvhodnější pro systémy vyžadující dlouhodobé nasazení a maximální stabilitu.
- Vydání CD (Continuous Delivery) 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

“Plánování vašeho prostředí IBM MQ na systému z/OS” na stránce 141
Při plánování vašeho prostředí IBM MQ musíte vzít v úvahu požadavky na prostředky pro datové sady, sady stránek, Db2, Prostředky párování a potřebu protokolování a zálohování zařízení. Pomocí tohoto tématu můžete naplánovat prostředí, ve kterém je spuštěn produkt IBM MQ .

Ujistěte se, že zprávy nejsou ztraceny (protokolování)

Dostupnost, obnova a restartování

Související úlohy

Kontrola požadavků

IBM MQ typy vydání: aspekty plánování

V systému IBM MQ 9.0 existují dva hlavní typy vydání: vydání Long Term Support (LTS) a vydání 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 9.2. Jeden obsahuje obrazy instalace pro vydání produktu IBM MQ 9.2.0 Long Term Support a druhý obrazy instalace pro vydání produktu IBM MQ 9.2.x Continuous Delivery . Stáhněte obrazy instalace z eAssembly podle vašeho výběru vydání.

Všechny verze produktu IBM MQ a verze produktu IBM MQ 9.2 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 metrikami cen. To znamená, že si můžete svobodně vybrat mezi obrazy instalace produktu LTS release a CD release pro produkt IBM MQ 9.2.

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 9.2.0 LTS a IBM MQ 9.2.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 9.2jsou 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 vydání CD v oddělených cílových zónách.
- Udržovat oddělené cílové a distribuční knihovny pro obě vydání

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 LTS vydání na CD vydání 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.

V 9.2.0 V 9.2.0 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 9.2.0 LTS, vypnout a spustit na adrese IBM MQ for z/OS 9.2.0 CD, vypnout a spustit na adrese IBM MQ for z/OS 9.2.0 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.

V 9.2.0 V 9.2.0 Tato schopnost je zachována pro vydání systému LTS a ta vydání systému CD s modifikátorem `0` , jako např. 9.2.0 CD, ale není možná, pokud je zdrojem nebo cílem migrace vydání produktu CD s nenulovým číslem modifikátoru, například 9.1.5 nebo 9.2.1.

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

Zdrojové vydání	Cílové vydání	Notes
8.0.0 LTS	9.2.0 LTS nebo 9.2.0 CD	Zpětná migrace není podporována, protože 8.0.0 LTS nemá standardní podporu.
9.0.0 LTS	9.2.0 LTS nebo 9.2.0 CD	Zpětná migrace je podporována.
9.1.0 LTS	9.2.0 LTS nebo 9.2.0 CD	Zpětná migrace je podporována.
9.1.5 CD	9.2.0 LTS nebo 9.2.0 CD	Zpětná migrace není podporována jako zdrojové vydání je CD s nenulovým modifikátorem.
V 9.2.0 9.2.0 LTS nebo V 9.2.0 9.2.0 CD	9.2.1 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 9.2

IBM MQ a IBM MQ Appliance místní aspekty připravenosti na GDPR

Pro PID:

- 5724-H72 IBM MQ
- 5655-AV9 IBM MQ Advanced for z/OS
- 5655-AV1 IBM MQ Advanced for z/OS Value Unit Edition
- 5655-AM9 IBM MQ Advanced Message Security for z/OS
- 5725-Z09 IBM MQ Appliance M2001
- 5737-H47 IBM MQ Appliance M2002
- 5655-MQ9 IBM MQ for z/OS
- 5655-VU9 IBM MQ for z/OS Value Unit Edition

- 5655-MF9 IBM MQ Managed File Transfer for z/OS
- 5655-ADV IBM WebSphere MQ Advanced for z/OS
- 5655-AMS IBM WebSphere MQ Advanced Message Security for z/OS
- 5724-A39 IBM WebSphere MQ for HP NonStop Server
- 5655-W97 IBM WebSphere MQ for z/OS
- 5655-VU8 IBM WebSphere MQ for z/OS Value Unit Edition
- 5655-VUE IBM WebSphere MQ for z/OS Value Unit Edition
- 5655-MFT IBM WebSphere MQ Managed File Transfer for z/OS

Upozornění:

Tento dokument je zamýšlen jako pomoc při přípravě vaší připravenosti na GDPR. Poskytuje informace o funkcích produktu IBM MQ , které můžete konfigurovat, a o aspektech použití produktu, které byste měli zvážit, abyste pomohli vaší organizaci s připraveností na GDPR. Tato informace není vyčerpávajícím seznamem z důvodu mnoha způsobů, jakým mohou klienti vybrat a konfigurovat funkce, a z širokého spektra způsobů, jak lze produkt použít samostatně a s aplikacemi a systémy třetích stran.

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

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

Obsah

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 sama 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 oborových 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 vložit 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 rozhraní JMS 2.0 , která umožňuje doručování zpráv do místa určení v budoucnu. 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.
- K ochraně obsahu adresáře použitého k ukládání protokolů trasování použijte šifrování na úrovni souboru nebo svazku.
- 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

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 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)
- IBM Cloud Pak for Integration Integrace řídicího panelu operací, který odesílá data trasování vysoké úrovně do centrálního zdroje (pouzeCP4I).
- 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]

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)

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 token LTPA2).
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 webovou konzolu: Jednotné přihlášení 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
- Protokoly 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 poskytnout 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 Uživatelé a role konzoly

Monitorování dat

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

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

Přečtěte si více:

- Monitorování sítě IBM MQ
- Služby zpráv diagnostiky
- QMErrorLog
- IBM MQ 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 IBM MQ architektury zahrnují konfiguraci a použití jednoho správce front.

Před plánováním architektury produktu IBM MQ se seznamte se základními koncepty produktu IBM MQ . Viz IBM MQ Technical overview.

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

- “Jednotlivý správce front s lokálními aplikacemi, které přistupují ke službě” na stránce 18

- “Jediný správce front se vzdálenými aplikacemi, které přistupují ke službě jako klienti” na stránce 18
- “Jednotlivý správce front s konfigurací publikování/odběru” na stránce 18

Jednotlivý správce front s lokálními aplikacemi, které přistupují ke službě

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

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

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

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

Jednotlivý správce front s konfigurací publikování/odběru

Alternativní architekturou, která používá jednoho správce front, je použít konfiguraci publikování/odběru. V systému zpráv typu publikování/odběr můžete oddělit poskytovatele informací od spotřebitelů dané informace. Liší se od bodu k bodového stylu systému zpráv v dříve popsaných architekturách, kde aplikace musí znát informace o cílové aplikaci, například název fronty, na které se mají zprávy vkládat. Při použití IBM MQ publish/Subscribe odesílající aplikace publikuje zprávu se zadaným tématem na základě předmětu informací. Produkt IBM MQ zpracovává distribuci zprávy aplikacím, které zaregistrovaly zájem o toto téma prostřednictvím odběru. Přijímající aplikace také nepotřebují vědět nic o zdroji zpráv, které mají být přijímány. Další informace 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.

Vytváření a správa správců front na více platformách

Architektury založené na více správcích front

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

Před plánováním architektury produktu IBM MQ se seznamte se základními koncepty produktu IBM MQ . Viz IBM MQ Technical overview.

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

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

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

Informace o vysoké úrovni pro plánování sítě IBM MQ naleznete v tématu “Navrhování distribuovaných sítí správce front” na stránce 20.

Informace o tom, jak plánovat kanály pro architekturu IBM MQ , najdete v tématu IBM MQ technologie distribuovaných front.

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

Související 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.

Vytváření a správa správců front na více platformách

Plánování vašich distribuovaných front a klastrů

Fronty můžete ručně připojit k distribuovaným správcům front nebo můžete vytvořit klastr správců front a nechat produkt, aby pro vás správce front připojil správce front. Chcete-li zvolit vhodnou topologii pro distribuovanou síť distribuovaných zpráv, musíte zvážit své požadavky na ruční řízení, velikost sítě, četnost změn, dostupnost a rozšiřitelnost.

Než začnete

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

Informace o této úloze

Chcete-li vytvořit distribuovanou síť systému zpráv, můžete ručně konfigurovat kanály pro připojení front, jejichž hostitelem je jiný správce front, nebo můžete vytvořit klastr správců front. Klastrování umožňuje správcům front komunikovat mezi sebou bez nutnosti nastavit další definice kanálů nebo definice vzdálených front, a zjednodušit tak jejich konfiguraci a správu.

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

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

Procedura

- Zvažte, kolik manuální ovládání potřebujete přes spojení ve vaší síti.

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

  Potřebujete-li více správců front, kteří spolu logicky souvisejí, a které potřebují sdílet data a aplikace, měli byste je seskupit do klastru správců front.
- Odhadněte, jak velká by vaše síť měla být.
  a) Odhadněte počet správců front, které potřebujete. Mějte na paměti, že fronty mohou být provozovány 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 náročné a měli byste zvážit použití klastru.

- Zvažte, jak bude dynamická aktivita sítě.

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

  Pokud očekáváte, že fronty budou často vytvářeny a odstraňovány, zvažte použití klastru.
- Zvažte své požadavky na dostupnost a rozšiřitelnost.
  a) Rozhodněte se, zda je třeba zajistit vysokou dostupnost správců front. Je-li tomu tak, odhadněte, kolik správců front se tento požadavek týká.
  b) Zvažte, zda některé z vašich správců front jsou méně schopné než jiné.
  c) Zvažte, zda jsou komunikační odkazy na některé z vašich správců front křehčí než u ostatních.
  d) Zvažte hostování front ve více správcích front.

  Ručně konfigurované sítě a klastry mohou být konfigurovány tak, aby byly vysoce dostupné a přizpůsobitelné. Používáte-li klastr, je třeba definovat dva další správce front jako úplná úložiště. Použití dvou úplných úložišť zajišťuje, že klastr bude fungovat i v případě, že se jedna z úplných úložišť stane nedostupnou. Ujistěte se, že správci front úplného úložiště jsou robustní, výkonní a mají dobrou síťovou konektivitu. Neplánujte používat správce front úplného úložiště pro jakoukoli jinou práci.
- Na základě těchto výpočtů můžete použít poskytnuté odkazy, které vám pomohou rozhodnout se, zda ručně nakonfigurovat připojení mezi správci front nebo použít klastr.

Jak pokračovat dále

Nyní jste připraveni konfigurovat distribuovanou síť systému zpráv.

Související úlohy

Konfigurace distribuovaných front

Konfigurace klastru správce front

Navrhování distribuovaných sítí správce front

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

Kanály lze vytvořit mezi vaším systémem a libovolným jiným systémem, se kterým potřebujete mít komunikaci. Vícepřechodové kanály lze vytvořit pro připojení k systémům, kde nemáte žádná přímá připojení. Připojení kanálu zpráv popsaná ve scénářích se zobrazují jako síťový diagram v produktu Obrázek 1 na stránce 21.

Potřebujete-li vytvořit kanály mezi systémy v různých fyzických sítích nebo kanály, které komunikují přes ochrannou bariéru, 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

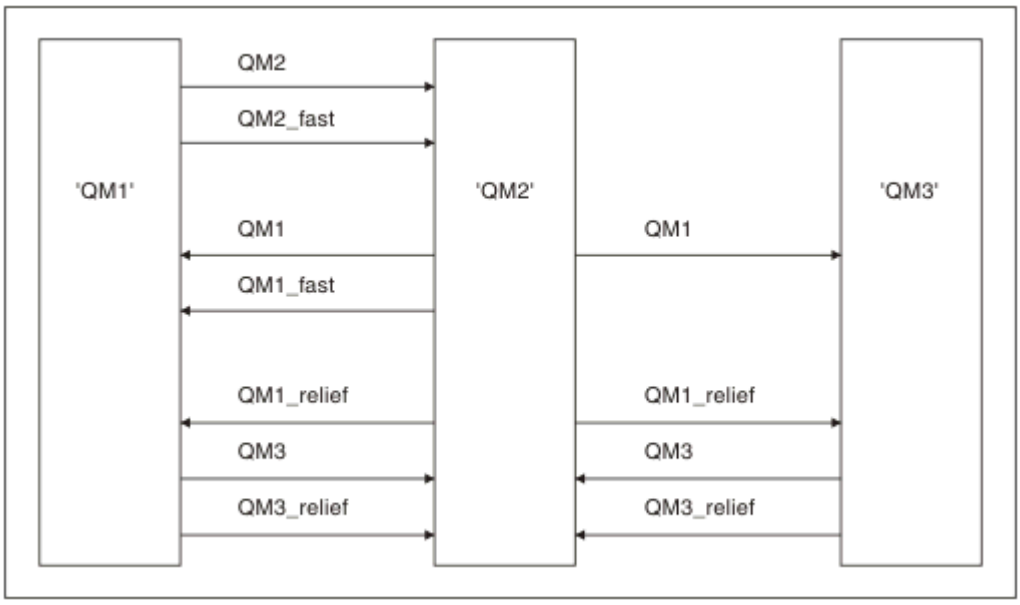
Přenosovým frontám může být přidělen libovolný název. Aby se však předešlo nejasnostem, můžete jim podle potřeby zadat stejné názvy jako názvy správce cílové fronty nebo názvy alias správce front. To asociuje přenosovou frontu s trasou, kterou používají, což poskytuje jasný přehled paralelních tras vytvořených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

Pro názvy kanálů není to tak clear-cut. Názvy kanálů v produktu Obrázek 1 na stránce 21 pro QM2, například, musí být odlišné pro příchozí a odchozí kanály. Všechny názvy kanálů mohou stále obsahovat názvy jejich přenosových front, ale musí být kvalifikovány, aby je bylo možné je označit jako jedinečné.

Například v QM2existuje kanál QM3 pocházející z QM1a kanál QM3 do systému QM3. Chcete-li, aby názvy byly jedinečné, může být první z nich pojmenován QM3_from_QM1a druhý může mít název

QM3_from_QM2. Tímto způsobem názvy kanálů zobrazují název přenosové fronty v první části názvu. Směr a sousedící název správce front jsou zobrazeny v druhé části názvu.

V produktu Tabulka 1 na stránce 21je uvedena tabulka s doporučenými názvy kanálů pro produkt Obrázek 1 na stránce 21 .



Obrázek 1. Diagram sítě zobrazující všechny kanály

Tabulka 1. Příklad názvů kanálů

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

Poznámka:

1. z/OS V systému IBM MQ for z/OSjsou názvy správců front omezeny na čtyři znaky.
2. Pojmenujte všechny kanály v síti jedinečně. Jak je zobrazeno v Tabulka 1 na stránce 21, včetně názvů zdrojového a cílového správce front v názvu kanálu je dobrý způsob, jak to provést.

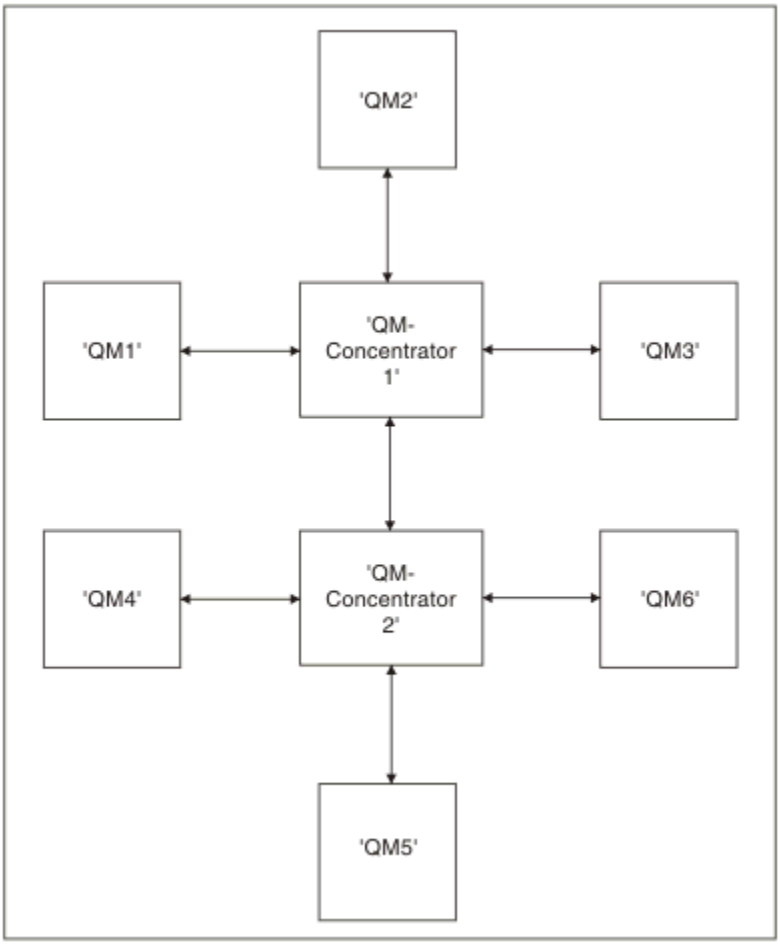
Plánovač sítě

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

U široce používaných aplikací je hospodárnější přemýšlet o lokálních přístupových místech pro koncentraci přenosu zpráv pomocí širokopásmových propojení mezi místními přístupovými servery, jak je zobrazeno v Obrázek 2 na stránce 22.

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

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



Obrázek 2. Diagram sítě ukazující QM-koncentrátory

Navrhování klastrů

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

Než začnete

Úvod do problematiky klastrování najdete v následujících tématech:

- Distribuované fronty a klastry
- "Porovnání klastrování a distribuovaných front" na stránce 29
- Komponenty klastru

Když navrhujete klastr správců front, musíte provést některá rozhodnutí. Nejprve se musíte rozhodnout, kteří správci front v klastru mají uchovávat úplná úložiště informací o klastru. Jakýkoli správce front, kterého vytvoříte, může pracovat v klastru. Pro tento účel si můžete vybrat libovolný počet správců front, ale ideální počet je dva. Informace o výběru správců front za účelem zadržení úplných úložišť naleznete v tématu "Jak vybrat správce front klastru k uchování úplných úložišť" na stránce 31.

Další informace o návrhu klastru naleznete v následujících tématech:

- "Ukázkové 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
- "Překrývání klastrů" na stránce 34

Jak pokračovat dále

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

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

Další informace, které vám pomohou při konfiguraci klastru, najdete v tématu"Rady pro klastrování" na stránce 35.

Plánování způsobu použití více přenosových front klastru

Můžete výslovně definovat přenosové fronty, nebo nechat systém generovat přenosové fronty pro 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

Definují se dvě metody definování přenosových front:

- Automaticky s použitím atributu DEFCLXQ správce front použijte tento postup:

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

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

  Funkce DEFCLXQ (CHANNEL) označuje, že každý odesílací kanál klastru standardně 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 tím, že definujete přenosovou frontu s hodnotou uvedenou pro atribut CLCHNAME. Atribut CLCHNAME označuje, které odesílací kanály klastru by měly používat přenosovou frontu. Další informace viz "Plánování pro ručně definované přenosové fronty klastru" na stránce 26.

Jaké zabezpečení potřebuji?

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

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

Kdy je vhodná doba na realizaci této změny?

Při změně přenosové fronty používané odesílacími kanály klastru je třeba přidělit čas, ve kterém má být aktualizace provedena, s uvážením následujících bodů:

- Čas požadovaný pro přepnutí přenosové fronty na kanál závisí na celkovém počtu zpráv ve staré přenosové frontě, kolik zpráv je třeba přesunout, a velikost zpráv.
- Aplikace mohou pokračovat v ukládání zpráv do přenosové fronty, zatímco se změna provádí. To může vést ke zvýšení času přechodu.
- Parametr CLCHNAME jakékoli přenosové fronty nebo DEFCLXQ můžete kdykoli změnit, nejlépe když je pracovní zátěž nízká.

  Všimněte si, že nic se nestane okamžitě.
- Změny se projeví až po spuštění nebo restartu kanálu. Když kanál spustí, zkontroluje aktuální konfiguraci a v případě potřeby přepne na novou přenosovou frontu.
- Existuje několik změn, které mohou změnit přidružení odesílacího kanálu klastru k přenosové frontě:
  - Pozměnění hodnoty atributu CLCHNAME přenosové fronty, což činí CLCHNAME méně specifické nebo prázdné.
  - Změna hodnoty atributu CLCHNAME přenosové fronty tak, aby byla hodnota CLCHNAME specifičtější.
  - Vymazává se fronta s uvedeným CLCHNAME.
  - Změna atributu DEFCLXQ správce front.

Jak dlouho to bude trvat?

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

U front obsahujících několik tisíc zpráv by mělo za sekundu trvat, než se zprávy přesunou. Skutečný čas závisí na počtu a velikosti zpráv. Váš správce front by měl být schopen přesunout zprávy po mnoha megabajtech za sekundu.

Aplikace mohou pokračovat v ukládání zpráv do přenosové fronty, zatímco se změna provádí. To může vést ke zvýšení času přechodu.

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

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

Jak implementovat změnu

Podrobnosti o tom, jak provést změnu na více přenosových front klastru, buď automaticky, nebo ručně, najdete v tématu Implementace systému pomocí více přenosových front klastru .

Zrušení provedení změny

Podrobné informace o vrácení změn, pokud narazíte na problémy, najdete v tématu Zrušení provedení změny .

Automaticky definované přenosové fronty klastru
Můžete nechat systém generovat přenosové fronty pro vás.

Informace o této úloze

Pokud kanál nemá ručně definovanou přenosovou frontu klastru, která je k němu přidružená, a vy uvedete DEFCLXQ (CHANNEL), pak 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 fronty pro přenos dynamického klastru s názvem SYSTEM.CLUSTER.TRANSMIT.ChannelName.

z/OS Chcete-li nastavit přenosové fronty klastru ručně, prohlédněte si téma "Plánování pro ručně definované přenosové fronty klastru" na stránce 26.

Důležité: z/OS

Je-li správce front migrován do produktu IBM MQ 8.0, správce front nemá SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE.

Nejprve definujte tuto frontu, aby se nabyl 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 naleznete v tématu ALTER QMGR.

Existují dvě volby:

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

CHANNEL
Znamená to, že používáte více přenosových front klastru.

2. Chcete-li přepnout na nové přidružení:
   - 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 aplikací jsou vloženy do původní definice.

   Když počet zpráv ve staré frontě dosáhne nuly, nové zprávy se umístí přímo do nové přenosové fronty.
3. Chcete-li monitorovat, kdy proces přepnutí skončí:
   a) Přepínač přenosové fronty, který je iniciován kanálem, běží na pozadí a váš administrátor může monitorovat protokol úlohy správce front, aby určil, kdy byl dokončen.
   b) Monitorujte zprávy v protokolu úlohy, abyste zobrazili průběh přepínače.
   c) Chcete-li se ujistit, že pouze kanály, které jste chtěli, používají tuto přenosovou frontu, 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 řekne, jaké nevyřízené změny jsou nevyřízené, a kolik zpráv je třeba přesunout mezi přenosové fronty.

Výsledky

Nastavili jste svou přenosovou frontu klastru nebo frontu.

Související úlohy
“Plánování pro ručně definované přenosové fronty klastru” na stránce 26
Pokud definujete přenosové fronty sami, máte větší kontrolu nad definicemi a sadu stránek, na které jsou zprávy zadrženy.

Související odkazy
ZMĚNIT QMGR
ZOBRAZIT CLUQMGR

Plánování pro ručně definované přenosové fronty klastru
Pokud definujete přenosové fronty sami, máte větší kontrolu nad definicemi a sadu stránek, na které jsou zprávy zadrženy.

Informace o této úloze

Váš administrátor ručně definuje přenosovou frontu a používá nový atribut CLCHNAME k definování toho, který odesílací kanál klastru nebo kanály budou tuto frontu používat jako přenosovou frontu.

Všimněte si, že CLCHNAME může zahrnovat zástupný znak na začátku nebo na konci, aby se jedna fronta mohla použít pro více kanálů.

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

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: Je třeba naplánovat, která sada stránek (a fond vyrovnávacích pamětí) se používá pro přenosové fronty. Můžete mít různé sady stránek pro různé fronty a zajistit izolaci mezi nimi, takže jedna sada stránek se zaplňuje, neovlivní přenosové fronty v jiných sadách stránek.

Informace o tom, jak každý kanál vybírá příslušnou frontu, najdete v tématu Práce s frontami přenosu klastru a odesílacími kanály klastru .

Když se kanál spustí, přepne své přidružení na novou přenosovou frontu. Aby nedošlo ke ztrátě zprávy, bude správce front automaticky přenášet zprávy ze staré přenosové fronty klastru do nové přenosové fronty v pořadí.

2. Použijte funkci CSQUTIL SWITCH, chcete-li provést změnu na nové přidružení.

   Další informace naleznete v tématu Přepnutí přenosové fronty přidružené k odesílacím kanálům klastru (SWITCH) .

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

      Příklad:

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

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

   c) Použijte funkci SWITCH k přepnutí zpráv nebo monitorování toho, co se děje.

      Použijte příkaz

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

      pro přesun zpráv 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 přenosovým kanálům klastru (SWITCH).

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

     – Použití příkazu SWITCH CHANNEL (*) poskytuje jednoduchý způsob, jak identifikovat stav přepínání odesílacích kanálů klastru. Umožňuje administrátorovi zjistit, jaké kanály se aktuálně přepíná, a kanály s nevyřízeným přepínačem, které se projeví při příštím spuštění těchto kanálů.

       Bez této schopnosti musí váš administrátor použít více příkazů DISPLAY a následně zpracovat výsledný výstup a zjistit tyto informace. Váš administrátor může také potvrdit, že změna konfigurace má požadovaný výsledek.

     – Je-li CSQUTIL použit k inicializaci přepínače, CSQUTIL bude pokračovat v monitorování průběhu této operace a končí pouze v případě, že byl přepínač dokončen.

To může výrazně usnadnit provádění těchto operací v dávkovém zpracování. Také pokud se CSQUTIL spustí pro přepínání více kanálů, CSQUTIL provede tyto akce postupně; to může mít menší dopad na váš podnik, než je více přepínačů spuštěných paralelně.

Výsledky

Nastavili jste svou přenosovou frontu klastru nebo frontu.

Řízení přístupu a více přenosových front klastru

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

IBM MQ vám dává možnost lokální a vzdálené kontroly, zda má uživatel oprávnění k vložení zprávy do vzdálené fronty. Typická aplikace IBM MQ používá pouze lokální kontrolu a spoléhá na správce vzdálené fronty, který důvěřuje kontrolám přístupu provedeného v lokálním správci front. Není-li použita vzdálená kontrola, zpráva se umístí do cílové fronty s oprávněním ke vzdálenému procesu kanálu zpráv. Chcete-li použít vzdálenou kontrolu, musíte nastavit oprávnění vložení přijímajícího kanálu na kontext zabezpečení.

Lokální kontroly se provádějí proti frontě, kterou aplikace otevírá. V distribuovaném řazení do fronty aplikace obvykle otevře definici vzdálené fronty a dojde k pokusu o přístup k definici vzdálené fronty. Je-li zpráva vložena s celým záhlavím směrování, jsou kontroly provedeny v přenosové frontě. Pokud aplikace otevře frontu klastru, která není na lokálním správci front, neexistuje lokální objekt, který by bylo možné zkontrolovat. Kontrola řízení přístupu se provádí proti přenosové frontě klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Dokonce i u více přenosových front klastru jsou kontroly lokálního řízení přístupu pro vzdálené fronty klastru prováděny vůči produktu `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Výběr místní nebo vzdálené kontroly je výběr mezi dvěma extrémy. Kontrola na dálku je jemnější. Každý uživatel musí mít v každém správci front v klastru, který má být vložen do fronty klastru, mít profil řízení přístupu. Lokální kontrola je hrubě odstupňovaná. Každý uživatel potřebuje pouze jeden profil řízení přístupu pro přenosovou frontu klastru na správci front, ke kterému jsou připojeni. Pomocí tohoto profilu mohou zprávu vložit do libovolné fronty klastru v libovolném správci front v libovolném klastru.

Administrátoři mají jiný způsob, jak nastavit řízení přístupu pro fronty klastru. Pomocí příkazu **setmqaut** můžete vytvořit profil zabezpečení pro frontu klastru na libovolném správci front v klastru. Tento profil se projeví, pokud otevřete vzdálenou frontu klastru lokálně a uvedete pouze název fronty. Také můžete nastavit profil pro vzdáleného správce front. Pokud tak učiníte, může správce front zkontrolovat profil uživatele, který otevře frontu klastru, a to tak, že poskytne úplný název.

Nové profily fungují pouze v případě, že změníte oddíl správce front, **`ClusterQueueAccessControl`** na `RQMName`. Předvolba je `Xmitq`. Je třeba vytvořit profily pro všechny fronty klastru, které používají fronty klastru. Pokud změníte oddíl na `RQMName` , aniž byste vytvořili profily, aplikace se pravděpodobně nezdaří.

Tip: Kontrola přístupu k frontě klastru se nevztahuje na vzdálené fronty. Kontroly přístupu se stále provádějí proti místním definicím. Změny znamenají, že můžete postupovat podle stejného přístupu ke konfiguraci kontroly přístupu u front klastru a témat klastru. z/OS Změny také sbližují přístup ke kontrole přístupu pro fronty klastru s z/OS. Příkazy pro nastavení kontroly přístupu v systému z/OS jsou odlišné, ale kontrolují přístup k profilu spíše než proti samotnému objektu.

Související pojmy

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 46
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

Související úlohy

Nastavení `ClusterQueueAccessControl`

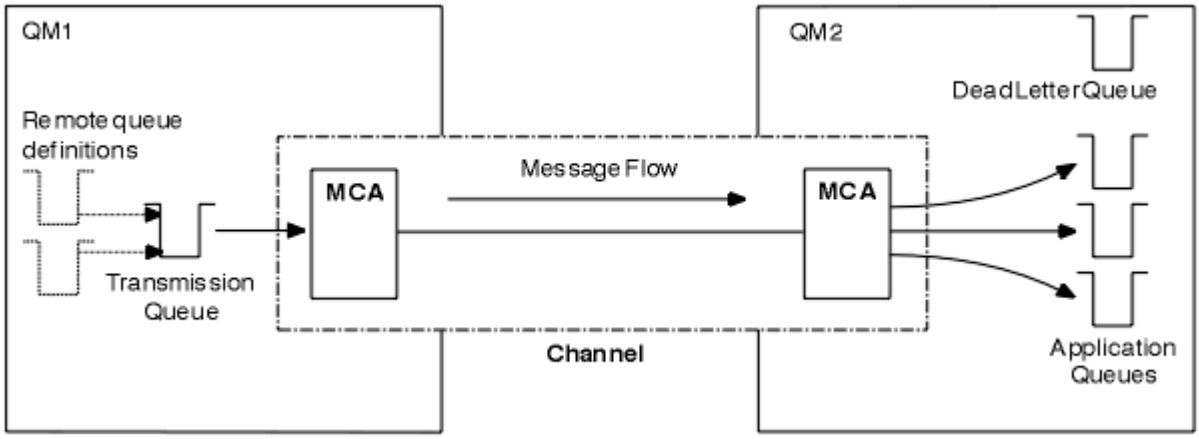
Porovnání klastrování a distribuovaných front

Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

Pokud nepoužíváte klastry, jsou vaši správci front nezávislí a komunikují pomocí distribuovaných front. Pokud jeden správce front potřebuje odeslat zprávy jinému uživateli, je třeba definovat následující údaje:

- Přenosová fronta
- Kanál pro vzdáleného správce front

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



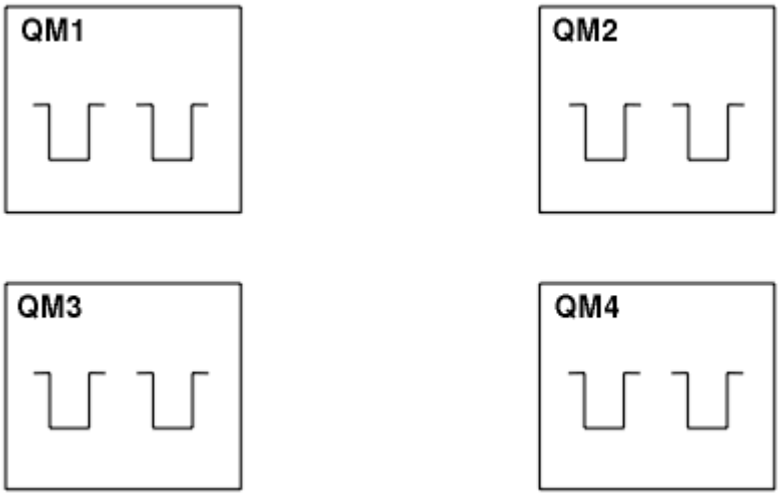
Obrázek 3. distribuované fronty

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 libovolnému jinému správci front ve stejném klastru bez explicitních definic. Neposkytujete definice kanálu, definice vzdálených front nebo přenosové fronty pro každý cíl. 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 potřebuje definovat pouze:

- jeden kanál příjemce klastru, na kterém mají být přijímány zprávy
- Jeden odesílací kanál klastru, se kterým se zavádí a učí se o klastru

Definice pro nastavení klastru oproti distribuovanému řazení do fronty

Podívejte se na Obrázek 4 na stránce 30, kde se zobrazují čtyři správci front s dvěma frontami. Uvažte, kolik definic je zapotřebí k připojení těchto správců front pomocí distribuovaných front. Porovnejte, kolik definic je třeba pro nastavení stejné sítě jako klastru.



Obrázek 4. Síť čtyř správců front

Definice pro nastavení sítě pomocí distribuovaných front

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

Tabulka 2. Definice pro distribuované ukládání do fronty

Popis	Počet na správce front	Celkový počet
Definice odesílacího kanálu pro kanál, do kterého mají být odesílány zprávy všem ostatním správcům front.	3	12
Definice přijímacího kanálu pro kanál, na kterém mají být přijímány zprávy od všech ostatních správců front.	3	12
Definice přenosové fronty pro přenosovou frontu ke každému jinému správci front	3	12
Definice lokální fronty pro každou lokální frontu	2	8
Definice vzdálených front pro každou vzdálenou frontu, do níž chce tento správce front vkládat zprávy.	6	24

Tento počet definic můžete snížit pomocí generických definic přijímacího kanálu. Maximální počet definic může být až 17 pro každého správce front, což je celkem 68 pro tuto síť.

Definice k nastavení sítě pomocí klastrů

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

Tabulka 3. Definice pro klastrování

Popis	Počet na správce front	Celkový počet
Definice odesílacího kanálu klastru pro kanál, v němž mají být odesílány zprávy do správce front úložiště	1	4
Definice přijímacího kanálu klastru pro kanál, na kterém mají být přijímány zprávy od jiných správců front v klastru	1	4

Tabulka 3. Definice pro klastrování (pokračování)		
Popis	**Počet na správce front**	**Celkový počet**
Definice lokální fronty pro každou lokální frontu	2	8

Chcete-li nastavit tento klastr správců front (se dvěma úplnými úložišti), budete potřebovat čtyři definice na každém správci front, což je celkem šestnáct definic. Je také třeba změnit definice správce front pro dva správce front a učinit z nich správci front úplného úložiště pro daný klastr.

Je vyžadována pouze jedna definice kanálu CLUSSDR a jedna definice kanálu CLUSRCVR . Je-li klastr definován, můžete přidávat nebo odebírat správce front (kromě správců front úložiště) bez narušení ostatních správců front.

Použití klastru snižuje počet definic potřebných k nastavení sítě, která obsahuje mnoho správců front.

Je-li méně definic, aby bylo méně riziko chyb:

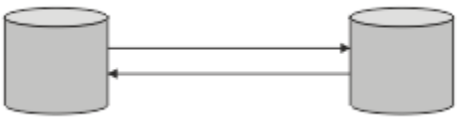
- Názvy objektů se vždy shodují, například jméno kanálu v páru odesilatel-příjemce.
- Název přenosové fronty zadaný v definici kanálu se vždy shoduje se správnou definicí přenosové fronty nebo názvem přenosové fronty, která je určena v definici vzdálené fronty.
- Definice QREMOTE vždy ukazuje na správnou 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 jakoukoli správu systému na kterémkoli jiném správci front. Není žádná možnost zapomenout na odstranění nebo upravit definice kanálu, vzdálené fronty nebo definice přenosové fronty. Do klastru můžete přidávat nové správce front bez jakéhokoli narušení existující sítě.

Jak vybrat správce front klastru k uchování úplných úložišť

V každém klastru si musíte vybrat alespoň jeden a nejlépe dva správce front, kteří budou uchovávat úplná úložiště. Dvě úplná úložiště jsou dostatečná pro všechny kromě těch výjimečných okolností. Je-li to možné, zvolte správce front, který je hostován na pevných a trvale připojených platformách, které nemají odpovídající výpadky, a které jsou na centrální pozici geograficky. Rovněž zvažte vyhrazení systémů jako hostitele úplných úložišť a nepoužívání těchto systémů pro žádné jiné úlohy.

Úplná úložiště jsou správci front, kteří udržují úplný obrázek o stavu klastru. Chcete-li tyto informace sdílet, je každé úplné úložiště připojeno pomocí kanálů CLUSSDR (a jejich odpovídajících definic CLUSRCVR) do všech ostatních úplných úložišť v klastru. Tyto kanály je třeba definovat ručně.



Obrázek 5. Dvě připojená úplná úložiště.

Každý další správce front v klastru udržuje obrázek o tom, co aktuálně ví o stavu klastru v *částečném úložišti*. Tito správci front publikují informace o sobě a žádají o informace o ostatních správcích front za použití jakýchkoli dvou dostupných úplných úložišť. Není-li vybrané úplné úložiště k dispozici, použije se další. Jakmile bude zvolené úplné úložiště opět dostupné, shromáždí nejnovější nové a změněné informace od ostatních, aby bylo možné pokračovat v kroku. Pokud všechna úplná úložiště nepůjdou mimo provoz, ostatní správci front použijí informace, které mají ve svých dílčích úložištích. Jsou však omezeny na používání informací, které mají; nové informace a požadavky na aktualizace nelze zpracovat. Když se úplná úložiště znovu připojí k síti, dochází k výměně zpráv za účelem uvedení všech úložišť (úplné i částečné) až do data.

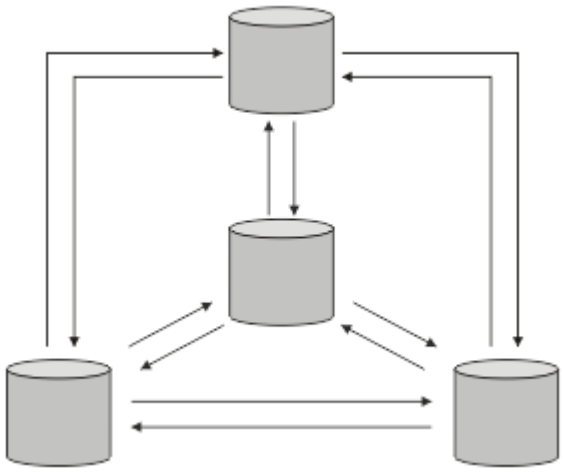
Při plánování přidělení úplných úložišť uveďte následující aspekty:

- Správci front, kteří byli vybráni k uchování úplných úložišť, musí být spolehliví a spravovaní. Zvolte správce front, kteří jsou hostováni na robustní a trvale připojené platformě.

- Zvažte plánované výpadky pro systémy, které jsou hostiteli vašich úplných úložišť, a ujistěte se, že se nekryjí výpadky.
- Zvažte výkon sítě: Zvolte správce front, kteří jsou geograficky v centrální poloze, nebo které sdílejí stejný systém jako ostatní správci front v klastru.
- Zvažte, zda je správce front členem více než jednoho klastru. Může být administrativně vhodné používat stejného správce front k hostování úplných úložišť pro několik klastrů, za předpokladu, že tento přínos je vyvážen podle toho, jak zaneprázdnění očekáváte, že správce front bude.
- Zvažte vyhrazení některých systémů, které mají obsahovat pouze úplná úložiště, a nikoli tyto systémy používat pro jiné úlohy. Tím je zajištěno, že tyto systémy vyžadují pouze údržbu konfigurace správce front a nebudou odebrány ze služby pro účely údržby jiných obchodních aplikací. Zajišťuje také, že úloha správy úložiště nebude soupeřit s aplikacemi pro systémové prostředky. To může být zvláště výhodné ve velkých klastrech (řekněme klastrů s více než 1000 správců front), kde úplná úložiště mají mnohem vyšší pracovní zátěž při správě stavu klastru.

S více než dvěma úplnými úložišti je to možné, ale zřídka se doporučuje. Ačkoli definice objektů (tj. fronty, témata a kanály) proudí do všech dostupných úplných úložišť, požadavky pouze proudí z dílčího úložiště do maxima dvou úplných úložišť. To znamená, že je-li definována více než dvě úplná úložiště a některá ze dvou úplných úložišť se stanou nedostupnými, některá dílčí úložiště nemusí přijímat aktualizace, které by očekávali. Viz MQ Clusters: Proč pouze dvě Úplná úložiště?

Jedna situace, ve které může být užitečné definovat více než dvou úplných úložišť, je při migraci existujících úplných úložišť na nový hardware nebo nové správce front. V takovém případě byste měli zavést nahrazující úplná úložiště a potvrdit, že byly zcela naplněny daty, než odeberete předchozí úplná úložiště. Při každém přidání celého úložiště nezapomeňte, že je třeba jej přímo připojit ke všem ostatním úplným úložištím prostřednictvím kanálů CLUSSDR .



Obrázek 6. Více než dvě připojená úplná úložiště

Související informace

MQ Clustery: Proč pouze dvě Úplná úložiště?

Jak velký může být klastr MQ ?

Uspořádání klastru

Vyberte, které správce front se mají spojit s úplným úložištěm. Zvažte vliv na výkon, verzi správce front a informace o tom, zda je žádoucí více kanálů CLUSSDR .

Pokud jste vybrali správce front k uchování úplných úložišť, musíte se rozhodnout, který správce front má odkazovat na které úplné úložiště. Definice kanálu CLUSSDR propojuje správce front s úplným úložištěm, ze kterého se nachází v ostatních úplných úložištích v klastru. Od té doby správce front odesílá zprávy do všech dvou úplných úložišť. Vždy se pokusí použít ten, ke kterému má nejprve definici kanálu CLUSSDR . Můžete se rozhodnout propojit správce front s úplným úložištěm. Při výběru si vezměte v úvahu topologii vaší konfigurace a fyzické nebo geografické umístění správců front.

Vzhledem k tomu, že všechny informace o klastru jsou odeslány do dvou úplných úložišť, mohou nastat situace, kdy chcete vytvořit druhou definici kanálu CLUSSDR . Druhý kanál CLUSSDR můžete definovat v klastru, který má mnoho úplných úložišť rozložená na celou šířku oblasti. Poté můžete řídit, do kterých dvou úplných úložišť budou vaše informace odeslány.

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 klastrové fronty 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 v rámci skupiny sdílení front může definovat lokální frontu, která má být sdílena až 32 správci front.

Sdílené fronty mohou být také fronty klastru. Kromě toho mohou být správci front ve skupině sdílení front také v jednom nebo 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 pokud se jednalo o tento případ, nebylo by možné zjistit, který správce front se má CLUSRCVR připojit ke každé z těchto časů. Fronty systému klastru, ve kterých se uchovávají informace o klastru, nejsou sdíleny. Každý správce front má své vlastní.

Kanály klastru se používají nejen k přenosu zpráv aplikace, ale k vnitřním systémovým zprávám o nastavení klastru. Každý správce front v klastru musí přijímat tyto interní systémové zprávy, aby se mohl řádně účastnit klastrování, takže potřebuje vlastní jedinečný kanál CLUSRCVR , na kterém je bude moci přijímat.

Sdílený CLUSRCVR může být spuštěn na libovolném správci front ve skupině sdílení front (QSG) a vést tak k nekonzistentní dodávce interních systémových zpráv pro správce front QSG, což znamená, že se žádný z nich nemůže řádně účastnit klastru. Chcete-li zajistit, že nebude možné použít sdílené kanály CLUSRCVR , jakýkoli pokus selže s chybovou zprávou CSQX502E .

Překrývání klastrů

Překrývající se klastry poskytují další administrativní schopnosti. Použijte seznamy názvů ke snížení počtu příkazů potřebných pro správu překrývajících se klastrů.

Klastry, které se překrývají, můžete vytvořit. Existuje mnoho důvodů, proč můžete definovat překrývající se klastry; například:

- Chcete-li umožnit různým organizacím, aby měly vlastní administraci.
- Umožněte administraci nezávislých aplikací samostatně.
- Vytvoření tříd služeb.

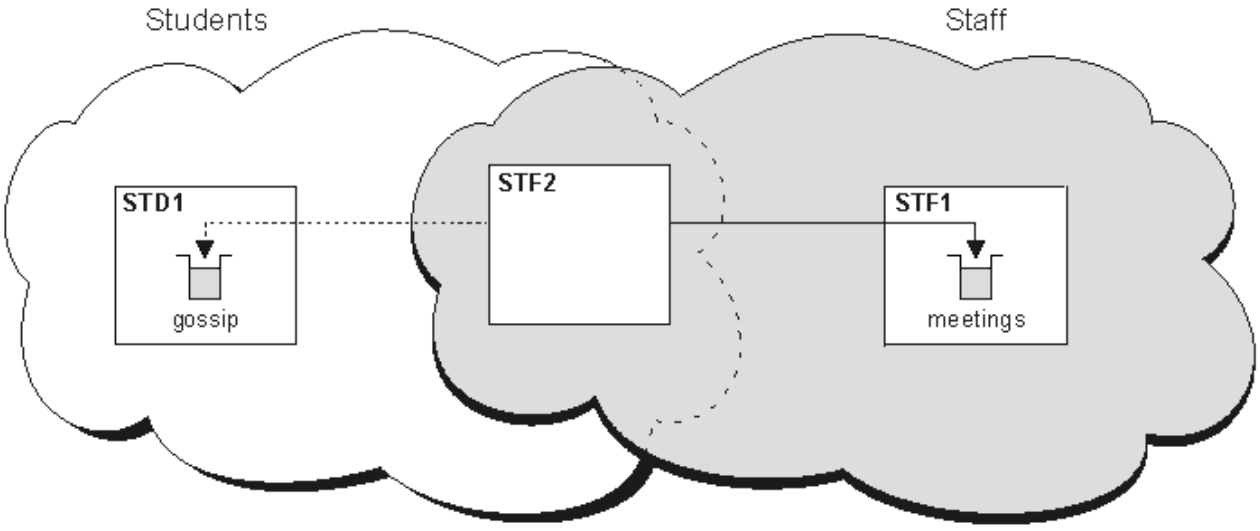
V produktu Obrázek 7 na stránce 35je správce front STF2 členem obou klastrů. Je-li správce front členem více než jednoho klastru, můžete využít výhody seznamů názvů a snížit počet definic, které potřebujete. Seznamy názvů obsahují seznam názvů, například názvy klastrů. Můžete vytvořit pojmenování seznamu názvů klastrů. Specify the namelist on the `ALTER QMGR` command for STF2 to make it a full repository queue manager for both clusters.

Máte-li ve vaší síti více klastrů, musíte jim dát odlišné názvy. Pokud se někdy sloučí dva klastry se stejným názvem, není možné je znovu oddělit. Je také dobrý nápad dát klastry a kanály různé názvy. Jsou snáze odlišeny, když se podíváte na výstup z příkazů `DISPLAY` . Názvy správců front musí být v rámci klastru jedinečné, aby mohl pracovat správně.

Definování tříd služeb

Představte si univerzitu, která má správce front pro každého zaměstnance a každého studenta. Zprávy mezi zaměstnanci mají cestovat do kanálů s vysokou prioritou a velkou šířkou pásma. Zprávy mezi studenty mají cestovat na levnější, pomalejší kanály. Tuto síť můžete nastavit pomocí tradičních technik distribuovaných front. Produkt IBM MQ vybírá kanály, které mají být použity, při pohledu na název cílové fronty a název správce front.

Chcete-li jasně rozlišovat mezi zaměstnanci a studenty, mohli byste jejich správce front seskupit do dvou klastrů, jak ukazuje Obrázek 7 na stránce 35. Produkt IBM MQ přesouvá zprávy do fronty schůzek v klastru personálu pouze prostřednictvím kanálů, které jsou definovány v daném klastru. Zprávy pro frontu pomluvy v klastru studentů přejdou přes kanály definované v daném klastru a přijmou odpovídající provozní třídu.



Obrázek 7. Třídy služeb

Rady pro klastrování

Možná budete muset provést některé změny v systémech nebo aplikacích před použitím klastrování. Jsou zde podobnosti i rozdíly oproti chování distribuovaných front.

- Chcete-li přistupovat k frontám klastru, je třeba přidat definice ručních konfigurací do správců front mimo klastr.
- Pokud sloučíte dva klastry se stejným názvem, nemůžete je oddělit znovu. Proto je vhodné poskytnout všem klastrům jedinečný název.
- Pokud zpráva dorazí do správce front, ale neexistuje žádná fronta, kterou by bylo možné přijmout, zpráva se umístí do fronty nedoručených zpráv. Pokud fronta nedoručených zpráv neexistuje, kanál

se znovu nezdaří a pokusí se o něj znovu. Použití fronty nedoručených zpráv je stejné jako u distribuovaných front.

- Integrita trvalých zpráv se udržuje. Zprávy nejsou duplikovány ani ztraceny jako výsledek použití klastrů.
- Použití klastrů snižuje administraci systému. Klastry usnadňují připojení větších sítí k mnoha dalším správcům front, než byste byli schopni uvažovat o použití distribuovaných front. Pokud se pokusíte povolit komunikaci mezi každým správcem front v klastru, hrozí nebezpečí, že budete spotřebovávat nadměrné síťové prostředky.
- Používáte-li produkt IBM MQ Explorer, který prezentuje správce front ve stromové struktuře, může být zobrazení velkých klastrů příliš náročné.
- Multi Účelem distribučních seznamů je použít jediný příkaz MQPUT k odeslání stejné zprávy do více míst určení. Distribuční seznamy jsou podporovány na IBM MQ for Multiplatforms. Můžete použít distribuční seznamy s klastry správců front. V klastru jsou všechny zprávy rozbaleny v čase MQPUT . Výhoda, co se týče síťového provozu, není tak velká jako v neklastrovém prostředí. Výhoda distribučních seznamů je taková, že četné kanály a přenosové fronty nemusí být definovány manuálně.
- Budete-li používat klastry pro vyvážení zátěže, prozkoumejte své aplikace. Zjistěte, zda vyžadují zprávy, které mají být zpracovány konkrétním správcem front nebo v určité posloupnosti. Takové žádosti mají mít spřízněnosti. Možná budete muset upravit aplikace dříve, než je budete moci používat ve složitých klastrech.
- Můžete se rozhodnout použít volbu MQOO_BIND_ON_OPEN na serveru MQOPEN k vynucení odeslání zpráv do určitého cíle. Není-li správce cílové fronty k dispozici, zprávy nebudou doručeny, dokud nebude správce front opět dostupný. Zprávy nejsou směrovány do jiného správce front kvůli riziku duplikace.
- Je-li správce front hostitelem úložiště klastrů, je třeba znát jeho název hostitele nebo adresu IP. Tyto informace musíte zadat do parametru CONNAME , když vytvoříte definici CLUSSDR v ostatních správcích front, které se připojují ke klastru. Jestliže používáte DHCP, je IP adresa předmětem změny, protože DHCP může alokovat novou IP adresu pokaždé, když restartujete systém. Proto v definicích CLUSSDR nesmíte uvést adresu IP. I v případě, že všechny definice CLUSSDR určují název hostitele a nikoli adresu IP, definice by stále nebyly spolehlivé. DHCP neaktualizuje nutně záznam adresáře DNS pro hostitele s novou adresou. Je-li třeba jmenovat správce front jako úplná úložiště v systémech, které používají DHCP, nainstalujte software, který zaručuje, aby byl adresář DNS aktuální.
- Nepoužívejte generická jména, například generické prostředky VTAM nebo generické názvy DNNS (Dynamic Domain Name Server) jako názvy připojení pro kanály. Pokud se tak stane, mohou se kanály připojovat k jinému správci front, než jste očekávali.
- Můžete získat zprávu pouze z lokální fronty klastru, ale můžete vložit zprávu do libovolné fronty v klastru. Pokud otevřete frontu pro použití příkazu MQGET , otevře správce front 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 přezkoumat aplikace a upravit je podle potřeby.
- Aktuální data monitorování a stavu pro kanál nebo frontu lze zobrazit pomocí příkazů DISPLAY CHSTATUS a DISPLAY QSTATUS **runmqsc** . Informace o monitorování lze použít k usnadnění měření výkonu a stavu systému. Monitorování je řízeno atributy správce front, fronty a kanálu. Monitorování automaticky definovaných odesílacích kanálů klastru je možné s atributem správce front MONACLS .

Související pojmy

Klastry

“Porovnání klastrování a distribuovaných front” na stránce 29

Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

Komponenty klastru

Související úlohy

Konfigurace klastru správce front

Nastavení nového klastru

Jak dlouho se uchovávají informace v úložištích správce front?

Úložiště správců front uchovávají informace po dobu 30 dnů. Automatický proces efektivně aktualizuje informace, které se používají.

Když správce front odešle nějaké informace o sobě, správci front úplného a dílčího úložiště uchovávají informace po dobu 30 dnů. Informace jsou odeslány například tehdy, když správce front oznámí vytvoření nové fronty. Chcete-li zabránit vypršení platnosti těchto informací, správci front automaticky po 27 dnech automaticky znovu odešlou všechny informace o sobě. Pokud částečné úložiště odešle nový požadavek na informace z části přes dobu 30 dnů, doba vypršení platnosti zůstane původní 30 dní.

Jakmile informace vyprší, nebude okamžitě z úložiště odebráno. Místo toho se koná za dobu odkladu 60 dnů. Není-li v době odkladu přijata žádná aktualizace, informace se odeberou. Doba odkladu umožňuje skutečnost, že správce front mohl být dočasně mimo službu v datu vypršení platnosti. Je-li správce front odpojen od klastru po dobu delší než 90 dnů, přestane být součástí klastru. Pokud se však znovu připojí k síti, stane se znovu součástí klastru. Úplná úložiště nevyužívají informace, jejichž platnost vypršela, aby vyhovělo novým požadavkům od jiných správců front.

Podobně platí, že pokud správce front odešle požadavek na informace o aktuální den z úplného úložiště, požadavek trvá 30 dní. Po 27 dnech IBM MQ zkontroluje požadavek. Pokud na něj bylo odkazováno během 27 dnů, dojde k jeho automatické aktualizaci. Pokud tomu tak není, je ponecháno na vypršení platnosti a správce front jej aktualizuje, pokud je znovu potřeba. Požadavky na vypršení platnosti zabrání tomu, aby nahromadění požadavků na informace z neaktivních správců front.

Poznámka: Měli byste stáhnout a nainstalovat opravu PTF pro operační systém APAR PH43191, který opravuje chyby systému při výpočtu doby vypršení platnosti odběru. Tyto chyby mohou způsobit předčasné vypršení platnosti odběru (výsledkem je zpráva CSQX456I) nebo vypršení platnosti po vypršení platnosti objektu (což má za následek chybné chyby MQRC 2085 (MQRC_UNKNOWN_OBJECT)).

U velkých klastrů může být rušivý, pokud mnoho správců front automaticky znovu odešle všechny informace o sobě ve stejnou dobu. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.

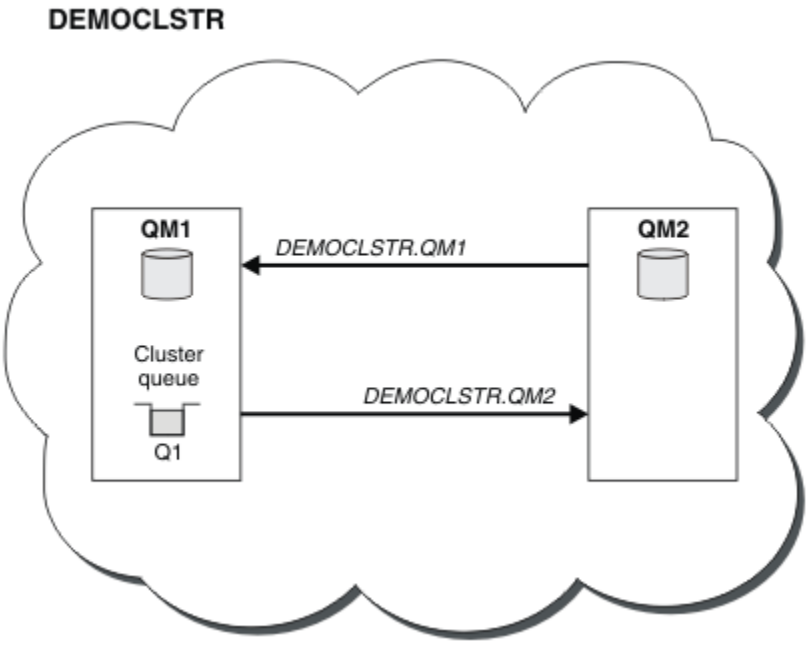
Související pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 67
Příkaz **REFRESH CLUSTER** se používá k zahození všech lokálně uložených informací o klastru a znovusestavení těchto informací z úplných úložišť v klastru. Tento příkaz byste neměli používat, kromě výjimečných okolností. Pokud ji potřebujete použít, musíte zvážit, jak ji budete používat. Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

Ukázkové klastry

První příklad ukazuje nejmenší možný klastr dvou správců front. Druhý a třetí příklad ukazuje dvě verze klastru správců front.

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



Obrázek 8. Malý klastr dvou správců front

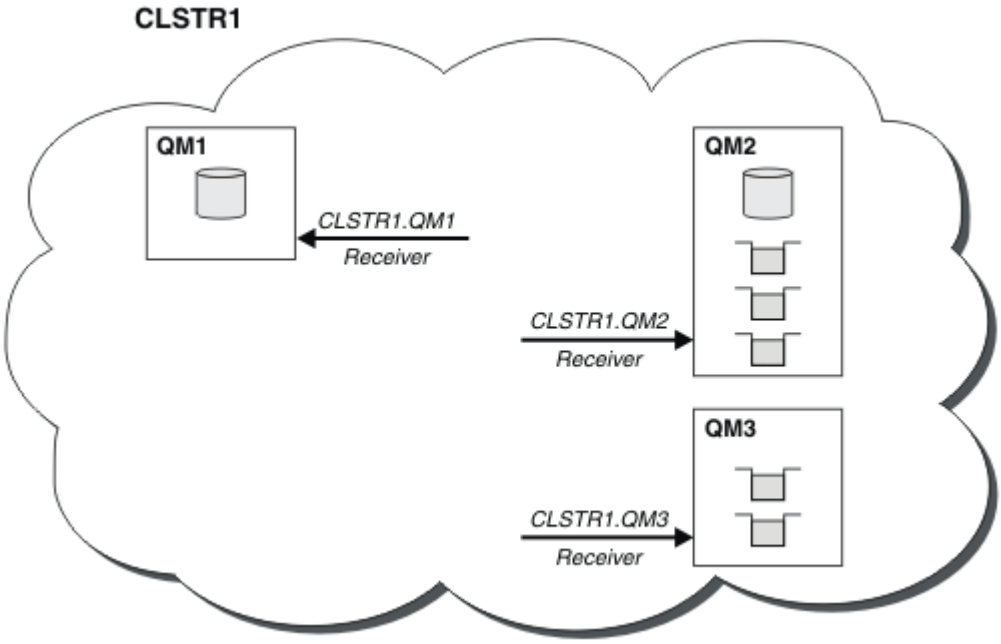
- Správci front mohou mít dlouhé názvy, jako například LONDON a NEWYORK. z/OS V systému IBM MQ for z/OSjsou názvy správců front omezeny na čtyři znaky.
- Každý správce front je obvykle konfigurován na samostatném počítači. Na stejném počítači však můžete mít více správců front.

Pokyny pro nastavení podobného vzorového klastru najdete 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.
- Hostitelská úložiště QM1 a QM2 informací o všech správcích front a objektech souvisejících s klastrem v klastru. Jsou označovány jako *správci front úplného úložiště*. Úložiště jsou znázorněna v diagramu stínovanými cylindry.
- QM2 a QM3 jsou hostiteli některých front, které jsou přístupné pro kteréhokoli jiného správce front v klastru. Fronty, které jsou dostupné pro kteréhokoli jiného správce front v klastru, se nazývají *fronty klastru*. Fronty klastru jsou znázorněny ve stínovaných frontách v diagramu. Fronty klastru jsou přístupné odkudkoli v klastru. Klastrový kód produktu IBM MQ zajišťuje, aby byly definice vzdálených front pro fronty klastru vytvořeny ve všech správcích front, které na ně odkazují.

  Stejně jako v případě distribuovaných front používá aplikace volání správce MQPUT k vložení zprávy do fronty klastru v libovolném správci front v klastru. Aplikace používá volání MQGET k načítání zpráv z fronty klastru pouze ve správci front, ve kterém je fronta umístěna.
- Každý správce front má ručně vytvořenou definici pro přijímající konec kanálu s názvem *cluster_name. queue_manager_name* , na kterém může přijímat zprávy. V přijímajícím správci front je *cluster_name. queue_manager_name* přijímajícím kanálem klastru. Přijímací kanál klastru je podobný přijímacímu kanálu používaném v distribuovaných frontách; přijímá zprávy pro správce front. Kromě toho také přijímá informace o klastru.

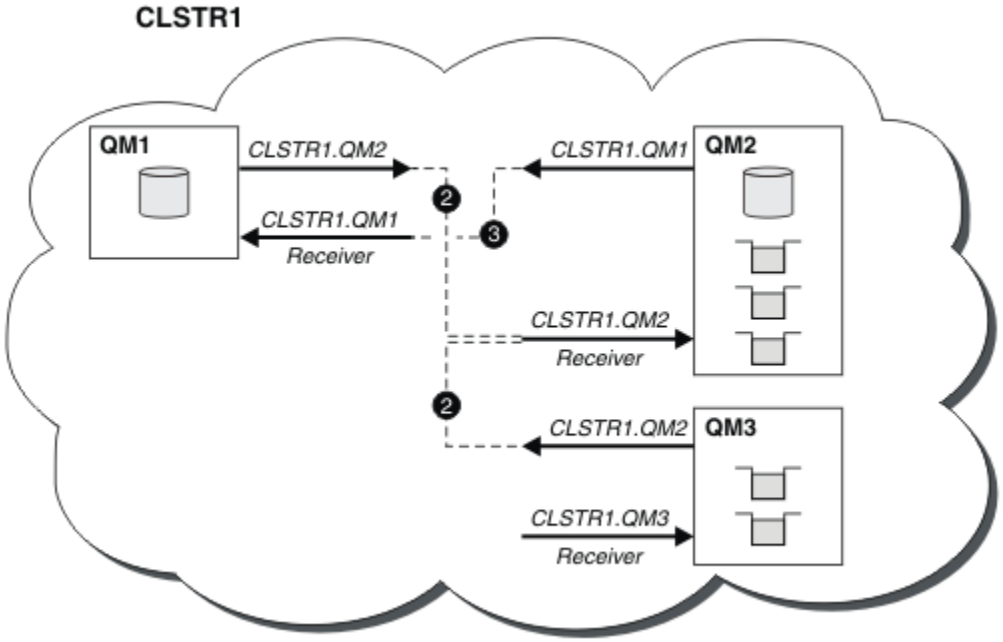


Obrázek 9. Klastr správců front

- V produktu Obrázek 10 na stránce 39 má každý správce front také definici pro odesílající konec kanálu. Připojuje se k přijímacímu kanálu klastru jednoho z správců front úplného úložiště. Na odesílajícím správci front je *cluster_name. queue_manager_name* odesílací kanál klastru. QM1 a QM3 mají odesílací kanály klastru připojující se k CLSTR1.QM2, viz tečkovaná čára "2".

  QM2 má odesílací kanál klastru, který se připojuje k CLSTR1.QM1, viz tečkovaná čára "3". Odesílací kanál klastru je jako odesílací kanál používaný v distribuovaných frontách; odesílá zprávy do přijímajícího správce front. Kromě toho také odesílá informace o klastru.

  Jakmile je definován koncový bod klastru a koncový bod odesílatele klastru, kanál se spustí automaticky.

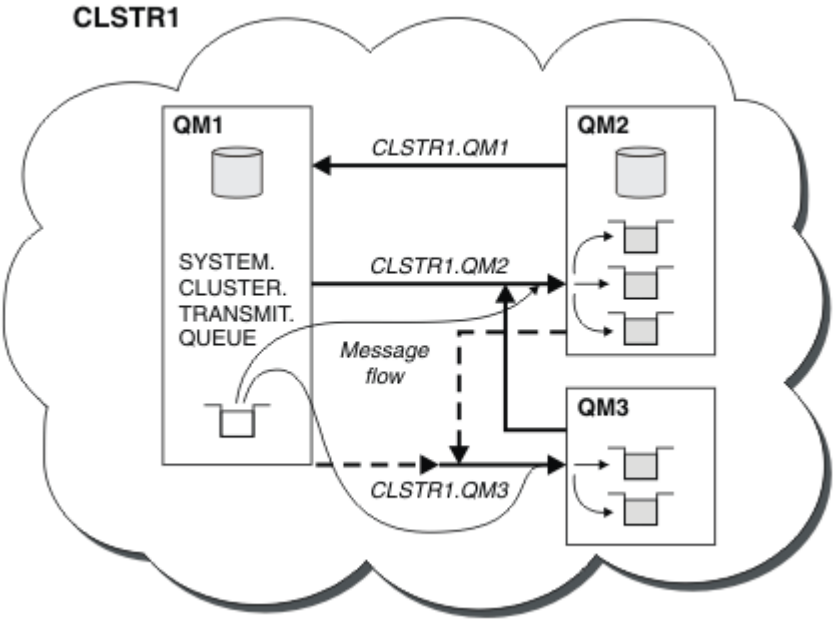


Obrázek 10. Klastr správců front s odesílacími kanály

Při definování kanálu odesílatele klastru v lokálním správci front bude tento správce front uveden v jednom z správců front úplného úložiště. Správce front úplného úložiště aktualizuje příslušným způsobem informace ve svém úplném úložišti. Poté dojde k automatickému vytvoření kanálu odesílatele klastru zpět k původnímu správci front a k odeslání informací správce front o daném klastru. Správce front se proto učí o klastru a klastru se dozví 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 produktu QM2. Když produkt QM3 poprvé musí přistupovat k těmto frontám, zjišťuje je prostřednictvím konzultací s úplným úložištěm. Úplné úložiště v tomto případě je QM2, k němuž se přistupuje pomocí odesílacího kanálu CLSTR1.QM2. S informacemi z úložiště může automaticky vytvořit vzdálené definice pro tyto fronty. Jsou-li fronty v systému QM1, tento mechanizmus stále funguje, protože produkt QM2 je úplné úložiště. Úplné úložiště má úplný záznam všech objektů v klastru. V tomto druhém případě by produkt QM3 také automaticky vytvořil kanál odesílatele klastru odpovídající kanálu příjemce klastru v systému QM1, který umožňuje přímou komunikaci mezi těmito dvěma servery.

Produkt 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 kanálem příjemce klastru CLSTR1.QM3. Zobrazuje také přenosovou frontu klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE, kterou produkt QM1 používá k odesílání zpráv. Všichni správci front v klastru mají přenosovou frontu klastru, ze které mohou odesílat zprávy libovolnému jinému správci front ve stejném klastru.



Obrázek 11. Klastr správců front zobrazující automaticky definované kanály

Poznámka: Další diagramy zobrazují pouze přijímající konce kanálů, pro které jste provedli ruční definice. Odesílající se konce vynechají, protože jsou většinou definovány automaticky podle potřeby. Automatická definice většiny kanálů odesílatele klastru je rozhodující pro funkci a efektivitu klastrů.

Související pojmy

“Porovnání klastrování a distribuovaných front” na stránce 29
Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

Komponenty klastru

Související úlohy

Konfigurace klastru správce front

Nastavení nového klastru

Klastrování: doporučené postupy

Klastry poskytují mechanizmus pro vzájemné připojení správců front. Doporučené postupy popsané v tomto oddílu jsou založeny na testování a zpětné vazbě od zákazníků.

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

Související pojmy

Distribuované fronty a klastry

Klastry

Související úlohy

“Navrhování klastrů” na stránce 22

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

Monitorování klastrů

Klastrování: Speciální pokyny pro překrývající se klastry

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

Vlastnictví klastru

Seznamte se se překrývajícími se klastry před čtením následujících informací. Informace o nezbytných informacích najdete v tématech “Překrývání klastrů” na stránce 34 a Konfigurace cest zpráv mezi klastry .

Při konfiguraci a správě systému, který se skládá ze překrývajících se klastrů, je nejlepší dodržet následující podmínky:

- Ačkoli jsou klastry produktu IBM MQ 'volně spojené', jak již bylo popsáno dříve, je užitečné považovat klastr jako jedinou jednotku administrace. Tento koncept se používá, protože interakce mezi definicemi na jednotlivých správcích front je kritická pro hladké fungování klastru. Příklad: Při použití front klastru s vyrovnáváním pracovní zátěže je důležité, aby jeden administrátor nebo tým pochopil úplnou sadu možných cílů pro zprávy, které závisí na definicích rozloženém v rámci klastru. Více triviálně musí být dvojice odesilatel/příjemce klastru kompatibilní v celém rozsahu.
- S ohledem na tento předchozí koncept; pokud se schází více klastrů (které mají být spravovány samostatnými týmy/jednotlivci), je důležité mít jasné zásady v místě řízení administrace správců front brány.
- Je užitečné zacházet s překrývajícími se klastry jako s jedním oborem názvů: Názvy kanálů a názvy správců front musí být jedinečné v rámci jediného klastru. Administrace je mnohem jednodušší, když je v celé topologii jedinečná. Nejlepší je následovat vhodnou konvenci pojmenování, možné konvence jsou popsány v “Konvence pojmenování klastrů” na stránce 33.
- Někdy je nezbytná spolupráce správy a správy systému: Například spolupráce mezi organizacemi, které vlastní různé klastry a které se musí překrývat. Jasné porozumění toho, kdo vlastní, a vynutitelné pravidla/konvence pomáhá klastrování při překrývání klastrů.

Překrývání klastrů: Komunikační brány

Obecně lze říci, že jeden klastr je snazší spravovat než více klastrů. Proto vytváření velkého počtu malých klastrů (například jedna pro každou aplikaci) je něco, čemu se lze vyhnout obecně.

Chcete-li však poskytnout třídy služeb, můžete implementovat překrývající se klastry. Příklad:

- Pokud máte soustředné klastry, kde je menší, pro publikování/odběr. Další informace naleznete v tématu Jak změnit velikost systémů .

- Mají-li být někteří správci front spravovány různými týmy. Další informace naleznete v předchozí části “Vlastnictví klastru” na stránce 41.
- Pokud má smysl z organizačního nebo geografického hlediska.
- Pokud ekvivalentní klastry pracují s rozlišováním názvů, například při implementaci TLS v existujícím klastru.

Neexistuje žádný přínos zabezpečení pro překrývající se klastry. Díky tomu, že klastry spravované dvěma různými týmy se překrývají, efektivně se spojí s týmy a také s topologií. Libovolné:

- Název inzerovaný v takovém klastru je přístupný pro druhý klastr.
- Název inzerovaný v jednom klastru může být inzerován na straně druhé, aby mohl čerpat vhodné zprávy.
- Neinzerovaný objekt ve správci front přilehlém k bráně může být vyřešen z libovolného klastru, jehož je brána členem.

Obor názvů je sjednocení obou klastrů a musí se s nimi zacházet jako s jedním oborem názvů. Proto je vlastnictví překrývajícího se klastru sdíleno mezi všemi administrátory obou klastrů.

Pokud systém obsahuje více klastrů, může existovat požadavek na směrování zpráv ze správců front v jednom klastru do front ve správcích front v jiném klastru. V této situaci je třeba vzájemně propojit více klastrů: Je dobrým vzorem, aby bylo možné sledovat použití správců front brány mezi klastry. Díky tomuto uspořádání se vyhýbá vytváření obtížně spravujících sítí dvoubodových kanálů a poskytuje dobré místo pro správu takových záležitostí, jako jsou bezpečnostní politiky. K dosažení tohoto uspořádání existují dva různé způsoby:

1. Zadejte jednoho (nebo více) správců front v obou klastrech s použitím druhé definice příjemce klastru. Toto uspořádání zahrnuje méně administrativních definic, ale jak bylo dříve uvedeno, znamená to, že vlastnictví překrývajícího se klastru je sdíleno mezi všemi administrátory obou klastrů.
2. Dvojice správců front v klastru s použitím správce front v klastru s použitím tradičních kanálů typu point-to-point.

V jednom z těchto případů lze použít různé nástroje pro správné směrování provozu. Aliasy fronty nebo správce front lze použít například k přesměrování do druhého klastru a alias správce front s prázdnou vlastností **RQMNAME** přepracuje vyrovnávání pracovní zátěže tam, kde je to požadováno.

Konvence pojmenování klastrů

Tyto informace obsahují předchozí pokyny k konvencím pojmenování a aktuální vodítko. Jak se technologie IBM MQ zlepšuje a zákazníci používají technologii novými nebo různými způsoby, nové doporučení a informace musí být poskytnuty pro tyto scénáře.

Konvence pojmenování klastru: Předchozí pokyny

Při nastavování nového klastru vezměte v úvahu konvenci pojmenování pro správce front. Každý správce front musí mít jiný název, ale může vám pomoci zapamatovat si, kteří správci front jsou seskupeni tam, kde jim dáte sadu podobných jmen.

Každý kanál příjemce klastru musí mít také jedinečný název.

Pokud máte více než jeden kanál ke stejnému správci front, každý s různými prioritami nebo pomocí různých protokolů, můžete rozšířit názvy tak, aby zahrnovaly různé protokoly; například `QM1.S1`, `QM1.N3a` `QM1.T4`. V tomto příkladě může být `S1` prvním kanálem SNA, `N3` může být kanál NetBIOS s prioritou sítě 3.

Konečný kvalifikátor může popisovat třídu služeb, kterou kanál poskytuje. Další informace naleznete v tématu Definování tříd služeb.

Nezapomeňte, že všechny odesílací kanály klastru mají stejný název jako jejich odpovídající přijímací kanál klastru.

Nepoužívejte generické názvy připojení ve vašich definicích příjemce klastru. V produktu IBM MQ for z/OSmůžete definovat generické prostředky VTAM nebo generické názvy *Dynamic Domain Name Server*

(DDNS), ale pokud používáte klastry, nedělejte to. Definujete-li CLUSRCVR s generickým **CONNAME**, neexistuje žádná záruka, že kanály CLUSSDR ukazují na správce front, kterého zamýšlíte. Počáteční CLUSSDR může skončit tím, že bude ukazovat na libovolného správce front ve skupině sdílení front, nikoli nutně v jednom hostiteli, který je hostitelem úplného úložiště. Dále, pokud kanál přejde do stavu opakování, může se znovu připojit k jinému správci front se stejným generickým názvem a tok vašich zpráv je přerušen.

Konvence pojmenování klastrů: Aktuální vedení

Předchozí pokyny v sekci “Konvence pojmenování klastru: Předchozí pokyny” na stránce 42jsou stále platné. Následující pokyny jsou však zamýšleno jako aktualizace při návrhu nových klastrů. Tento aktualizovaný návrh zajišťuje jedinečnost kanálů v rámci více klastrů, což umožňuje úspěšné překrytí více klastrů. Vzhledem k tomu, že správci front a klastry mohou mít názvy až 48 znaků a název kanálu je omezen na 20 znaků, je třeba při pojmenovávání objektů od začátku postupovat opatrně, aby nedošlo ke změně konvence pojmenování v polovině cesty projektem.

Při nastavování nového klastru vezměte v úvahu konvenci pojmenování pro správce front. Každý správce front musí mít jiný název. Pokud dáte správcům front v klastru sadu podobných názvů, může vám pomoci zapamatovat si, kteří správci front jsou seskupeni tam, kde.

Při definování kanálů mějte na paměti, že všechny automaticky vytvořené odesílací kanály klastru na libovolném správci front v klastru mají stejný název jako odpovídající kanál příjemce klastru konfigurovaný v přijímajícím správci front v klastru, a musí proto být jedinečný a dávat smysl v rámci klastru administrátorům daného klastru. Názvy kanálů jsou omezeny na maximálně 20 znaků.

Jednou z možností je použít název správce front, kterému předchází název klastru. Je-li například název klastru CLUSTER1 a správci front jsou QM1, QM2, pak kanály příjemce klastru jsou CLUSTER1.QM1, CLUSTER1.QM2.

Tuto konvenci můžete rozšířit, pokud kanály mají odlišné priority nebo používají různé protokoly; například `CLUSTER1.QM1.S1`, `CLUSTER1.QM1.N3`a `CLUSTER1.QM1.T4`. V tomto příkladě může být S1 prvním kanálem SNA, N3 může být kanál NetBIOS s prioritou sítě tří.

Konečný kvalifikátor může popisovat třídu služeb, kterou kanál poskytuje.

Aspekty produktu IBM MQ for z/OS

V produktu IBM MQ for z/OSmůžete definovat generické prostředky VTAM nebo generické názvy *Dynamic Domain Name Server* (DDNS). Názvy připojení můžete definovat pomocí generických názvů. Když však vytváříte definici příjemce klastru, nepoužívejte generický název připojení.

Problém s použitím generických názvů připojení pro definice příjemce klastru je následující. Pokud definujete parametr `CLUSRCVR` s generickým názvem `CONNAME` , neexistuje žádná záruka, že kanály `CLUSSDR` budou ukazovat na správce front, kterého zamýšlíte. Počáteční `CLUSSDR` může skončit tím, že bude ukazovat na libovolného správce front ve skupině sdílení front, nikoli nutně z hostitele, 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, které by narušilo tok zpráv.

Klastrování: Aspekty návrhu topologie
Toto téma obsahuje pokyny pro plánování a administraci klastrů IBM MQ . Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

Po přemýšlení o tom, kam uživatelské aplikace a interní administrativní procesy mají být umístěny v předstihu, je možné se vyvarovat mnoha problémům nebo minimalizovat v pozdějším termínu. Toto téma obsahuje informace o návrhu rozhodnutí, která mohou zlepšit výkon a zjednodušit úlohy údržby jako měřítka klastru.

- “Výkon klastrové infrastruktury” na stránce 44
- “Úplná úložiště” na stránce 44
- “Měly by aplikace používat fronty v úplných úložištích?” na stránce 45

- “Správa definic kanálů” na stránce 46
- “Vyrovnávání zátěže pomocí více kanálů” na stránce 46

Výkon klastrové infrastruktury

Když se aplikace pokusí otevřít frontu ve správci front v klastru, správce front zaregistruje svůj zájem o úplná úložiště pro danou frontu, aby se mohla zjistit, kde fronta v klastru existuje. Všechny aktualizace umístění nebo konfigurace fronty jsou automaticky odeslány úplným úložištěm do příslušného správce front. Tato registrace zájmu je interně známa jako odběr (tyto odběry nejsou stejné jako odběry produktu IBM MQ používané pro systém zpráv publikování/odběru v produktu IBM MQ).

Všechny informace o klastru procházejí všemi úplnými úložišti. Úplná úložiště jsou proto vždy používána v klastru pro provoz administrativní zprávy. Vysoké využití systémových prostředků při správě těchto odběrů a jejich přenos a výsledné konfigurační zprávy může způsobit značné zatížení na infrastruktuře klastrování. Existuje řada věcí, které je třeba vzít v úvahu při zajišťování toho, aby bylo toto zatížení chápáno a minimalizováno, kde je to možné:

- Čím více jednotlivých správců front používajících frontu klastru je, tím více odběrů je v systému, a tím větší administrativní režie při výskytu změn a je třeba upozornit odběratele, kteří mají zájem o upozornění, zejména na správce front úplného úložiště. Jedním způsobem, jak minimalizovat zbytečný provoz a načítání celého úložiště, je připojení podobných aplikací (tj. aplikací, které pracují se stejnými frontami), do menšího počtu správců front.
- Kromě počtu odběrů v systému, které ovlivňují výkon, může rychlost změn v konfiguraci klastrovaných objektů ovlivnit výkon, například časté změny konfigurace klastrovaných front.
- Je-li správce front členem více klastrů (tj. je součástí překrývajícího se systému klastru), každý z úroků ve frontě má za následek odběr pro každý klastr, jehož členem je, a to i v případě, že jsou správci front úplná úložiště pro více než jeden klastr. Toto uspořádání zvyšuje zatížení systému a je jedním z důvodů, proč zvážit, zda je více překrývajících se klastrů zapotřebí, spíše než jeden klastr.
- Přenosy zpráv aplikace (tj. zprávy odesílané aplikacemi produktu IBM MQ do front klastru) nepůjdou přes úplná úložiště, aby dosáhly cílových správců front. Tento přenos zpráv se odesílá přímo mezi správcem front, do kterého se zpráva vstupuje do klastru, a správcem front, ve kterém fronta klastru existuje. Proto není nutné přizpůsobit vysoké rychlosti přenosu zpráv aplikací s ohledem na správce front úplného úložiště, pokud správci front úplného úložiště nejsou uvedeni ani jedna z těchto dvou správců front. Z tohoto důvodu se doporučuje, aby se správci front úplného úložiště nepoužívali pro provoz zpráv aplikací v klastrech, kde je zátěž klastrové infrastruktury 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 najdete v tématu Úložiště klastru.

Úplná úložiště musí být uchovněna na serverech, které jsou spolehlivé a jsou vysoce 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 stále fungovat.

Podrobnosti o jakýchkoli aktualizacích prostředků klastru vytvořených správcem front v klastru; například klastrované fronty jsou odesílány z tohoto správce front do dvou úplných úložišť v nejvíce v daném klastru (nebo na jednom z nich, pokud v klastru existuje pouze jeden správce front úplného úložiště). Tato úplná úložiště uchovávají informace a šíří je do všech správců front v klastru, které zobrazují zájem o něj (tj. přihlásí se k odběru). Chcete-li zajistit, aby každý člen klastru měl k dispozici aktuální pohled na prostředky klastru, musí být každý správce front schopen komunikovat alespoň s jedním správcem front úplného úložiště v jednom okamžiku.

Pokud z jakéhokoli důvodu nemůže správce front komunikovat s žádnými úplnými úložišti, může v klastru pokračovat v práci na základě již uložené úrovně informací v mezipaměti po určitou dobu, ale nejsou k dispozici žádné nové aktualizace nebo přístup k dříve nepoužitým prostředkům klastru.

Z tohoto důvodu je třeba usilovat o to, aby byla všechna dostupná dvě úložiště dostupná po celou dobu. Toto uspořádání však neznamená, že by měla být přijata extrémní opatření, protože funkce klastru je bez úplného úložiště dostatečně krátká.

Existuje další důvod, proč klastr musí mít dva správce front úplného úložiště, kromě dostupnosti informací o klastru: Důvodem je zajistit, aby informace o klastru uchovávané v úplné mezipaměti úložiště existují ve dvou místech pro účely zotavení. Pokud existuje pouze jedno úplné úložiště a ztratí informace o klastru, pak je nutný ruční zásah na všech správcích front v rámci klastru, aby mohl klastr opět fungovat. Pokud však existují dvě úplná úložiště, pak proto, že informace jsou vždy publikovány a odebírany ze dvou úplných úložišť, může být neúspěšné úplné úložiště zotaveno s minimálním úsilím.

- Je možné provádět údržbu správců front úplného úložiště ve dvou úplných návrhových klastrech úložiště bez dopadu na uživatele klastru: Klastr bude nadále fungovat pouze s jedním úložištěm, takže je-li to možné, přiveďte úložiště dolů, použijte údržbu a zálohujete znovu jednu po druhé. I v případě, že dojde k výpadku v druhém úplném úložišti, spuštění aplikací nebude dosaženo minimálně po dobu tří dnů.
- Pokud neexistuje vhodný důvod pro použití třetího úložiště, jako například použití geograficky lokálního úplného úložiště geografických důvodů, použijte dva návrhy úložiště. Pokud máte tři úplná úložiště, znamená to, že nikdy nevíte, které z nich jsou aktuálně používány, a mohou existovat administrativní problémy způsobené 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 správce front s více instancemi nebo pomocí podpory vysoké dostupnosti specifické pro platformu, aby se zlepšila jejich dostupnost.
- Jste povinni plně propojit všechny správce front úplného úložiště s ručně definovaným odesílacím kanálem klastru. Zvláštní pozornost je třeba věnovat tomu, že klastr má z nějakého důvodu opodstatněný důvod více než dvě úplná úložiště. V této situaci je často možné ujít jeden nebo více kanálů a za to, že není okamžitě zřejmé. Když nedochází k úplnému propojení, často vznikají potíže při diagnostice problémů. Je těžké diagnostikovat, protože některá úplná úložiště neudržují všechna data úložiště, a proto jsou výsledkem správců front v klastru s různými pohledy na klastr, v závislosti na úplných úložištích, ke kterým se připojují.

Měly by aplikace používat fronty v úplných úložištích?

Úplné úložiště je ve většině způsobů přesně jako každý jiný správce front, a proto je možné hostitelské fronty aplikací v úplném úložišti hostovat a připojovat aplikace přímo k těmto správcům front. Měly by aplikace používat fronty v úplných úložištích?

Běžně přijímaná odpověď je "Ne?". I když je tato konfigurace možná, mnoho zákazníků preferuje udržet tyto správce front vyhrazené pro údržbu úplné mezipaměti klastru úložiště. Body, které je třeba vzít v úvahu při rozhodování o obou variantě, jsou zde popsány, ale v konečném důsledku musí být architektura klastru vhodná pro konkrétní požadavky daného prostředí.

- Přechody na vyšší verzi: Obvykle je třeba nejprve převést na vyšší verzi správce front úplného úložiště, aby bylo možné používat nové funkce klastru v nových verzích produktu IBM MQ pro správce front v úložišti. Když aplikace v klastru chce používat nové funkce, může být užitečné mít možnost aktualizovat úplná úložiště (a část dílčích úložišť) bez testování řady aplikací s funkcí.
- Údržba: Podobným způsobem, pokud musíte použít urgentní údržbu na úplná úložiště, je možné je restartovat nebo obnovit pomocí příkazu **REFRESH** , aniž by se aplikace dotýkala.
- Výkon: Jak rostou klastry a požadavky na údržbu mezipaměti klastru úplných úložišť jsou vyšší, udržování aplikací odděleně snižuje riziko ovlivnění výkonu aplikací díky soupeření o systémové prostředky.
- Hardwarové požadavky: Typicky úplná úložiště nemusí být silná; například jednoduchý server UNIX s dobrým očekáváním dostupnosti je dostatečný. Alternativně pro velmi velké nebo neustále se měnící klastry je třeba brát v úvahu výkon počítače plného úložiště.

- Softwarové požadavky: Požadavky jsou obvykle hlavním důvodem pro výběr hostitelských front aplikací v úplném úložišti. V malém klastru může kolokace znamenat požadavek na méně správců front/serverů pro všechny.

Správa definic kanálů

Dokonce i v rámci jednoho klastru může existovat více definic kanálů, která poskytuje více tras mezi dvěma správci front.

Někdy je výhodné mít v rámci jednoho klastru paralelní kanály, ale toto rozhodnutí o návrhu je třeba důkladně zvážit; kromě toho může mít tento návrh za následek nedostatečné využití kanálů, které snižuje výkon. Tato situace se vyskytne, protože testování obvykle zahrnuje odeslání zpráv ve konstantní rychlosti, takže jsou plně využity paralelní kanály. Ale s reálnými světovými podmínkami nestálého proudu zpráv, algoritmus vyrovnávání pracovní zátěže způsobuje pokles výkonu, protože tok zpráv je přepnut z kanálu na kanál.

Je-li správce front členem více klastrů, existuje volba pro použití jediné definice kanálu se seznamem názvů klastru, nikoli k definování samostatného kanálu produktu CLUSRCVR pro každý klastr. Toto nastavení však může způsobit potíže administrace později; zvažte například případ, kdy se TLS použije na jeden klastr, ale ne za sekundu. Proto je vhodné vytvořit oddělené definice a konvence pojmenování navržené v produktu “Konvence pojmenování klastrů” na stránce 33 to podporují.

Vyrovnávání zátěže pomocí více kanálů

Tyto informace jsou určeny jako rozšířené porozumění subjektu. Základní vysvětlení tohoto tématu (které je třeba chápat před použitím těchto informací) naleznete v tématu Použití klastrů pro správu pracovní zátěže, Vyrovnávání pracovní zátěže v klastrecha Algoritmus správy pracovní zátěže klastru.

Algoritmus správy pracovní zátěže klastru nabízí velkou sadu nástrojů, které však nesmí být všechny používány bez plného pochopení způsobu práce a interakce mezi nimi. Je možné, že není okamžitě zřejmé, jak se důležité kanály nacházejí v procesu vyrovnávání pracovní zátěže: Algoritmus správy zátěže round-robin se chová jako více aplikačních kanálů ke správci front, který vlastní klastrovanou frontu, a je s ní zacházeno jako s více instancemi této fronty. Tento proces je podrobněji vysvětlen v následujícím příkladu:

1. Jsou zde dva správci front, kteří jsou hostiteli fronty v klastru: QM1 a QM2.
2. K dispozici je pět kanálů příjemce klastru pro produkt QM1.
3. K dispozici je pouze jeden kanál příjemce klastru s QM2.
4. Když **MQPUT** nebo **MQOPEN** na QM3 zvolí instanci, algoritmus je pětkrát více pravděpodobné, že odešle zprávu do QM1 než QM2.
5. Situace v kroku 4 se vyskytne, protože algoritmus vidí šest voleb pro výběr z (5 + 1) a round-robins přes všech pět kanálů na QM1 a jeden kanál na QM2.

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

1. Při vkládání zpráv se algoritmus správy pracovní zátěže nepodívá do jednotlivých front klastru, podívá se na kanály klastru, které mohou dosáhnout těchto cílů.
2. Pro dosažení lokálních cílů jsou v tomto seznamu obsaženy lokální přijímací kanály (ačkoli se nepoužívají k odeslání zprávy).
3. Je-li zastaven lokální kanál příjemce, algoritmus správy pracovní zátěže preferuje při výchozím nastavení alternativní instanci, pokud není zastavena její CLUSRCVR. Pokud existuje více lokálních instancí CLUSRCVR pro místo určení a alespoň jedna není zastavena, zůstává lokální instance vhodná.

Klastrování: izolace aplikace pomocí více přenosových front klastru
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru

nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

Když implementujete aplikaci, máte možnost volby, které prostředky produktu IBM MQ sdílí s ostatními aplikacemi a které prostředky se nesdílejí. Existuje celá řada typů prostředků, které lze sdílet, přičemž hlavní jsou servery samotné, správce front, kanály a fronty. Můžete zvolit konfiguraci aplikací s menším počtem sdílených prostředků; alokací samostatných front, kanálů, správců front nebo dokonce serverů pro jednotlivé aplikace. Pokud tak učiníte, bude celková konfigurace systému mnohem větší a složitější. Použití klastru 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 48 je výseč velké implementace produktu IBM MQ , která ilustruje významnost sdílení SYSTEM.CLUSTER.TRANSMIT.QUEUE. V diagramu je aplikace, Client App, připojena ke správci front QM2 v klastru CL1. Zpráva od Client App je zpracována aplikací, Server App. Zpráva je načtena příkazem Server App z fronty klastru Q1 ve správci front QM3 v CLUSTER2. Vzhledem k tomu, že klientské a serverové aplikace nejsou ve stejném klastru, je zpráva přenesena správcem front brány QM1.

Normální způsob, jak nakonfigurovat bránu klastru, je vytvořit 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 dostupné ve všech klastrech. Zprávy vkládané do aliasů fronty klastru jsou směrovány přes správce front brány na správné místo určení. Správce front brány vloží zprávy odesílané do klastrovaných alias front do společného produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE v systému QM1.

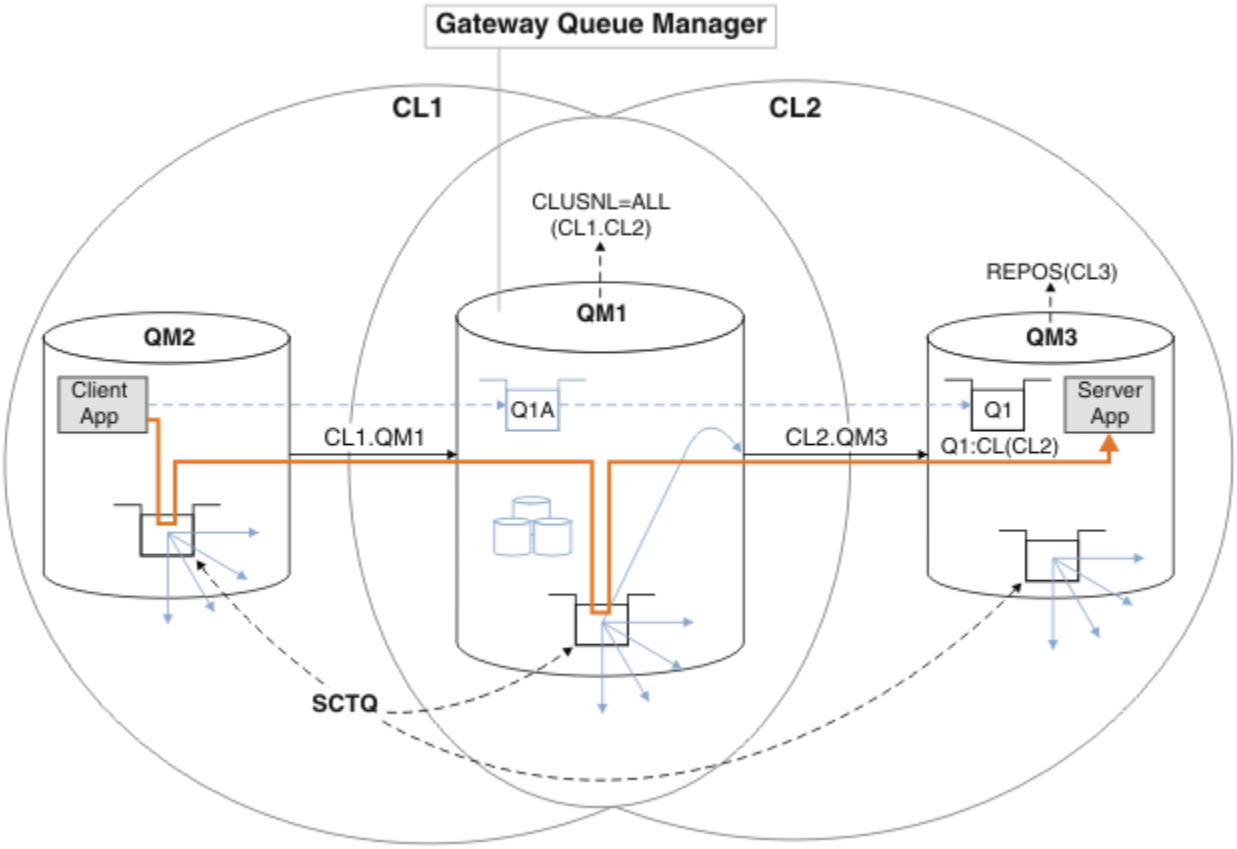
Architektura rozbočovače a paprsek vyžaduje všechny zprávy mezi klastry, které se mají předávat prostřednictvím správce front brány. Výsledkem je, že všechny zprávy procházejí přes jednu přenosovou frontu klastru v systému QM1, SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Z hlediska výkonu se nejedná o problém s jedinou frontou. Společná přenosová fronta obecně nereprezentuje 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 používají kanály.

Z některých jiných perspektiv má použití jediné přenosové fronty pro více aplikací nevýhody:

- Tok zpráv nelze izolovat do jednoho místa určení od toku zpráv do jiného cíle. Nemůžete oddělit úložiště zpráv před jejich přesměrovávat, i když jsou cíle v různých klastrech v různých správcích front.

  Pokud se jeden cíl klastru stane nedostupným, zprávy pro toto místo určení se zobrazí v jedné přenosové frontě a zprávy se nakonec zaplní. Jakmile je přenosová fronta plná, zastaví vkládání zpráv do přenosové fronty pro jakékoli místo určení klastru.
- Přenos zpráv do různých cílů klastru není snadný. Všechny zprávy jsou na jedné přenosové frontě. Zobrazení hloubky přenosové fronty vám dává málo informací o tom, zda jsou zprávy přenášeny do všech míst určení.



Poznámka: Šipky v Obrázek 12 na stránce 48 a následující čísla jsou různého typu. Pevné šipky představují toky zpráv. Popisky na pevných šipkách jsou názvy kanálů zpráv. Šedé pevné šipky představují potenciální toky zpráv z `SYSTEM.CLUSTER.TRANSMIT.QUEUE` do kanálů odesílatele klastru. Černá přerušovaná čára spojuje popisky s jejich cíli. Šedé šířené šipky jsou odkazy; například z volání `MQOPEN` z `Client App` do definice fronty aliasu klastru `Q1A`.

Obrázek 12. Aplikace Client-server implementovaná do rozbočovače a mluvila s architekturou pomocí klastrů produktu IBM MQ .

V produktu Obrázek 12 na stránce 48jsou klienti produktu `Server App` otevření fronty `Q1A`. Zprávy se umístí do `SYSTEM.CLUSTER.TRANSMIT.QUEUE` na `QM2`, přenesou se do `SYSTEM.CLUSTER.TRANSMIT.QUEUE` na `QM1`a pak jsou přeneseny do `Q1` na `QM3`, kde jsou přijímány aplikací `Server App` .

Zpráva z produktu `Client App` prochází přes přenosové fronty klastru systému v systémech `QM2` a `QM1`. V produktu Obrázek 12 na stránce 48je cílem izolovat tok zpráv od správce front brány od klientské aplikace, aby jeho zprávy nebyly uloženy v systému `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Toky můžete izolovat od všech ostatních klastrovaných správců front. Můžete také izolovat toky v opačném směru, zpět ke klientovi. Chcete-li uchovat popis řešení stručný, popisy považují pouze jeden tok z aplikace klienta.

Řešení pro izolaci provozu zpráv klastru ve správci front brány klastru

Jednou z možností k vyřešení problému je použití aliasů správce front nebo definic vzdálených front k přemostění mezi klastry. Vytvořte klastrované definice vzdálených front, přenosovou frontu a kanál, které oddělují jednotlivé toky zpráv ve správci front brány. Další informace naleznete v tématu Přidání definice vzdálené fronty k izolaci zpráv odeslaných ze správce front brány.

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

1. Definujte další přenosové fronty klastru ručně a definujte, které odesílací kanály klastru budou přenášet zprávy z jednotlivých přenosových front; viz téma Přidání přenosové fronty klastru za účelem izolování provozu zpráv klastru odeslaného ze správce front brány.
2. Umožněte správci front automaticky vytvářet a spravovat další přenosové fronty klastru. Definuje jinou přenosovou frontu klastru pro každý odesílací kanál klastru. Další informace naleznete v tématu Změna výchozí na oddělené přenosové fronty klastru k izolaci provozu zpráv.

Můžete sloučit ručně definované přenosové fronty klastru pro některé odesílací kanály klastru, přičemž správce front spravuje zbytek. Kombinace přenosových front je přístup použitý v části Přidání přenosové fronty klastru k izolování přenosu zpráv klastru odeslané ze správce front brány. V tomto řešení se většina zpráv mezi klastry používá běžnou 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.

Omezuje se pouze konfigurace v části Přidání přenosové fronty klastru za účelem izolace přenosu zpráv klastru odeslané ze správce front brány . Neoddělují provoz zpráv do fronty klastru ve stejném klastru ve stejném klastru jako jiná fronta klastru. Přenos zpráv do jednotlivých front můžete oddělit s použitím definic vzdálených front, které jsou součástí distribuovaných front. U klastrů, které používají více přenosových front klastru, můžete oddělit provoz zpráv, který bude směřovat do různých odesílacích kanálů klastru. Více front klastru ve stejném klastru, ve stejném správci front, sdílejí odesílací kanál klastru. Zprávy pro tyto fronty jsou uloženy ve stejné přenosové frontě před tím, než jsou přeposlána ze správce front brány. V konfiguraci v části Přidání klastru a přenosové fronty klastru k izolování přenosu zpráv klastru odeslaného ze správce front brányje omezení pro přidání jiného klastru a vytvoření nového klastru a člena nového klastru jako člena fronty klastru. Nový správce front může být jediným správcem front v klastru. Do klastru můžete přidat více správců front a pomocí stejného klastru izolovat fronty klastru také u těchto správců front.

Související pojmy

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

Práce s přenosovými frontami klastru a odesílacími kanály klastru

“Překrývání klastrů” na stránce 34
Překrývající se klastry poskytují další administrativní schopnosti. Použijte seznamy názvů ke snížení počtu příkazů potřebných pro správu překrývajících se klastrů.

Související úlohy

Autorizace vkládání zpráv ve vzdálených frontách klastru

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

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

Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány

Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu 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
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty.

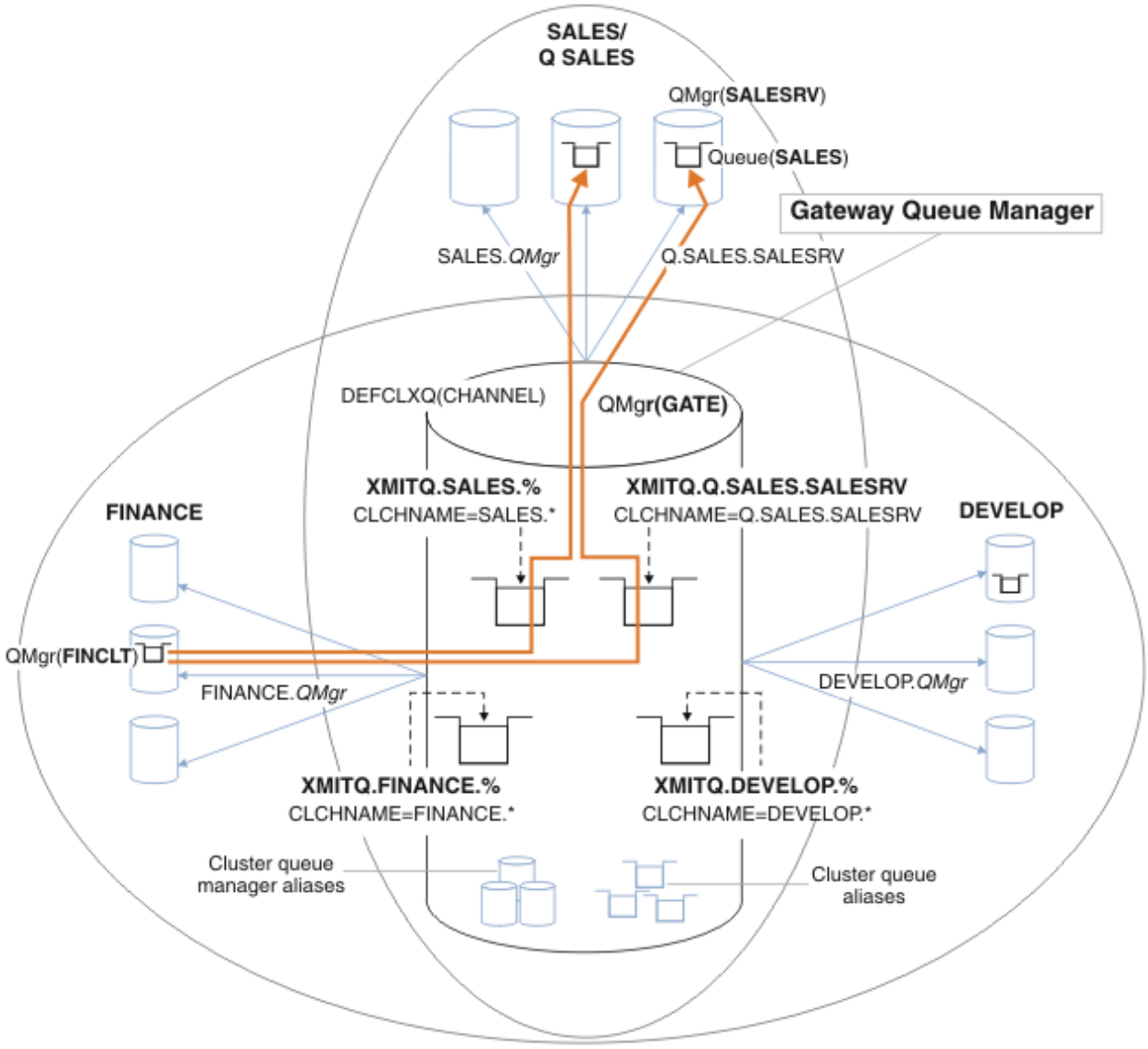
Než začnete

Zkontrolujte “Jak se rozhodnout, jaký typ přenosové fronty klastru použít” na stránce 52.

Informace o této úloze

Při plánování toho, jak nakonfigurovat správce front pro výběr přenosové fronty klastru, máte k dispozici určité volby.

1. Jaká je výchozí přenosová fronta klastru pro přenosy zpráv klastru?
   a. Společná přenosová fronta klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.
   b. Oddělit přenosové fronty klastru. Správce front spravuje oddělené přenosové fronty klastru. Vytvoří 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 nakonfigurovat ručně. V tomto případě nastavte atribut fronty **CLCHNAME** přenosové fronty na název kanálu odesílatele klastru. Vyberte odesílací kanál klastru, který má přenášet zprávy z této přenosové fronty.
   b. Kombinujte provoz zpráv pro skupinu odesílacích kanálů klastru do stejné přenosové fronty klastru, viz Obrázek 13 na stránce 51. V tomto případě nastavte atribut fronty **CLCHNAME** každé společné přenosové fronty na generický název kanálu odesílatele klastru. Generický název kanálu odesílatele klastru je filtr pro seskupení názvů odesílacích kanálů klastru. Například skupina `SALES.*` seskupuje všechny kanály odesílatele klastru, jejichž názvy začínají řetězcem `SALES.`. Do řetězce filtru můžete umístit více zástupných znaků. Zástupný znak je hvězdička, "`*`". Představuje od nuly po libovolný počet znaků.



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

Postup

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

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

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

2. Izolovat jakékoli toky zpráv, které nesmí sdílet přenosovou frontu klastru s jinými toky.
   - Viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 54. V příkladu je to fronta SALES , která musí být izolována, je členem klastru SALES , na SALESRV. Chcete-li izolovat frontu SALES , vytvořte nový klastr Q . SALES, vytvořte člena SALESRV správce front a upravte frontu SALES tak, aby patřila do produktu Q . SALES.
   - Správci front, kteří odesílají zprávy do produktu SALES , musí být zároveň členy nového klastru. Pokud používáte alias klastrované fronty a správce front brány jako v příkladu, můžete v mnoha případech omezit změny, aby správce front brány mohl být členem nového klastru.

- Oddělením toků od brány k cíli však do brány ze zdrojového správce front neoddělují toky. Ale občas se ukáže, že stačí k oddělení toků od brány a ne toku do brány. Pokud to není dostatečné, přidejte do nového klastru zdrojového správce front. Pokud chcete, aby zprávy cestovali přes bránu, přesuňte alias klastru do nového klastru a pokračujte v odesílání zpráv na alias klastru na bráně a nikoli přímo do cílového správce front.

Chcete-li izolovat toky zpráv, postupujte takto:

a) Konfigurujte cíle toků tak, aby každá cílová fronta byla jedinou frontou v konkrétním klastru, v daném správci front.

b) Vytvořte odesílací kanály klastru a příjemce klastru pro všechny nové klastry, které jste vytvořili podle systematického pojmenování.

- Viz “Klastrování: Speciální pokyny pro překrývající se klastry” na stránce 41.

c) Definujte přenosovou frontu klastru pro každý izolovaný cíl na každém správci front, který odesílá zprávy do cílové fronty.

- Konvence pojmenování pro přenosové fronty klastru je použít hodnotu atributu názvu kanálu klastru, `CLCHNAME`, s předponou `XMITQ.`

3. Vytvořte přenosové fronty klastru, které budou odpovídat požadavkům řízení nebo monitorování.

- Typické řízení a požadavky na monitorování mají za následek přenosovou frontu na klastr nebo přenosovou frontu na správce front. Pokud postupujete podle konvence pojmenování pro kanály klastru, *`ClusterName.  QueueManagerName`*, je snadné vytvořit generické názvy kanálů, které vyberou klastr správců front nebo všechny klastry, jejichž členem je správce front; viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 54.
- Rozšiřte konvence pojmenování pro přenosové fronty klastru tak, aby vyhovdily generickým názvům kanálů, nahrazením symbolu hvězdičky znakem procent. 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, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na `SYSTEM.CLUSTER.TRANSMIT.QUEUE`, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

“Překrývání klastrů” na stránce 34
Překrývající se klastry poskytují další administrativní schopnosti. Použijte seznamy názvů ke snížení počtu příkazů potřebných pro správu překrývajících se klastrů.

Související úlohy

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

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

Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány

Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv

Vytvoření dvou překrývajících se klastrů se správcem front brány

Konfigurace cest zpráv mezi klastry

Jak se rozhodnout, jaký typ přenosové fronty klastru použít
Jak si vybrat mezi různými volbami konfigurace přenosové fronty klastru.

Počínaje produktem IBM WebSphere MQ 7.5 můžete zvolit, která přenosová fronta klastru je přidružena ke kanálu odesílatele klastru.

1. Můžete mít všechny odesílací kanály klastru přidružené k jedné výchozí přenosové frontě klastru, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Tato volba je výchozí a je jedinou volbou pro správce front, kteří běží IBM WebSphere MQ 7.1nebo starší.
2. Všechny odesílací kanály klastru můžete nastavit tak, aby byly automaticky přidruženy k samostatné 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 vysílací frontu s jedinečným názvem v případě, že je atribut správce front **DEFCLXQ** nastaven na hodnotu CHANNEL.

   Upozornění: Používáte-li vyhrazenou hodnotu SYSTEM.CLUSTER.TRANSMIT.QUEUES se správcem front, který byl upgradován z verze produktu starší než IBM WebSphere MQ 7.5, ujistěte se, že má SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE volbu SHARE/NOSHARE nastavenou na hodnotu **SHARE**.
3. Můžete nastavit konkrétní odesílací kanály klastru, které mají být obsluhovány jednou přenosovou frontou klastru. Vyberte tuto volbu tak, že vytvoříte přenosovou frontu a nastavíte její atribut **CLCHNAME** na název kanálu odesílatele klastru.
4. Můžete vybrat skupiny odesílacích kanálů klastru, které mají být obsluhovány jednou přenosovou frontou klastru. Vyberte tuto volbu tak, že vytvoříte přenosovou frontu a nastavíte její atribut **CLCHNAME** na generický název kanálu, jako například *ClusterName*.*. Pokud pojmenujete kanály klastru podle následujících konvencí pojmenování v produktu “Klastrování: Speciální pokyny pro překrývající se klastry” na stránce 41, tento název vybere všechny kanály klastru připojené ke správcům front v klastru *ClusterName*.

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

Doporučené postupy

Ve většině případů je výchozí konfigurací nejlepší volbou pro existující instalace produktu IBM MQ . Správce front klastru ukládá zprávy klastru do jedné přenosové fronty klastru, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Máte možnost změnit výchozí nastavení na 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 konfiguraci. Proces přepnutí z výchozí konfigurace na alternativní výchozí nastavení pro jednu přenosovou frontu pro každý odesílací kanál klastru je automatický. Přepínání zpět je také automatické. Volba jednoho nebo druhého není kritická, můžete ji změnit.

Důvodem pro výběr jiné konfigurace je více práce s řízením a správou, než s funkcemi či výkonem. U několika výjimek nevyužívá konfigurace více přenosových front klastru chování správce front. Výsledkem je více front a vyžaduje, abyste upravili procedury monitorování a správy, které jste již nastavili, odkazujte na jednotlivou přenosovou frontu. To je důvod, proč je zůstatek, který zůstává s výchozí konfigurací, nejlepší volbou, pokud nemáte silnou správu věcí veřejných nebo řízení pro jinou volbu.

Výjimky jsou znepokojeni tím, co se stane, pokud se zvýší počet zpráv uložených ve SYSTEM.CLUSTER.TRANSMIT.QUEUE . Pokud každý krok oddělíte zprávy pro jedno místo určení ze zpráv pro jiné místo určení, pak problémy kanálu a doručení s jedním místem určení by neměly mít vliv na doručení do jiného cíle. Počet zpráv uložených v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE se však může zvýšit kvůli nedoruzpůsobování zpráv dostatečně rychle do jednoho místa určení. Počet zpráv v systému SYSTEM.CLUSTER.TRANSMIT.QUEUE pro jedno místo určení může ovlivnit doručování zpráv do jiných míst určení.

Chcete-li se vyhnout problémům, které vznikají při zaplnění jedné přenosové fronty, je cílem vytvořit dostatečnou kapacitu pro vaši konfiguraci. Pokud dojde k selhání místa určení a ke spuštění nevyřízených požadavků na zprávu, budete mít k dispozici čas na vyřešení problému.

Pokud jsou zprávy směrovány přes centrální správce front, jako je například přenosová brána klastru, sdílejí společnou přenosovou frontu SYSTEM.CLUSTER.TRANSMIT.QUEUE. Pokud počet zpráv uložených ve správci front v produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE ve správci front brány dosáhne své

maximální hloubky, správce front začne odmítat nové zprávy pro přenosovou frontu, dokud nedojde ke snížení její hloubky. Přetížení ovlivňuje zprávy pro všechna místa určení, která jsou směrována přes bránu. Zprávy zálohují přenosové fronty ostatních správců front, kteří odesílají zprávy do komunikační brány. Problém se projevuje ve zprávách zapisovaných do protokolů chyb správce front, klesající propustnosti zpráv a uplynulé doby mezi odesláním zprávy a časem, kdy zpráva dorazí do místa určení.

Vliv přetížení na jednotlivé přenosové fronty může být zřejmý, i před tím, než je plný. Pokud máte smíšený přenos zpráv a některé velké přechodné zprávy a některé malé zprávy, doba pro doručení malých zpráv se zvýší, když se zaplní přenosová fronta. Zpoždění je způsobeno zápisem velkých přechodných zpráv na disk, které by normálně nebyly zapsány na disk. Pokud máte kritické toky zpráv, sdílíte přenosovou frontu klustru s jinými smíšenými toky se smíšenými zprávami, může být vhodné nakonfigurovat speciální cestu zpráv k izolaci od jiných toků zpráv; viz téma Přidání klastru a fronty vysílání klastru za účelem izolace přenosu zpráv klastru odeslané ze správce front brány.

Dalším důvodem pro konfiguraci samostatných přenosových front klastru je splnění požadavků řízení nebo zjednodušení monitorování zpráv, které jsou odesílány do různých cílů klastru. Můžete například demonstrovat, že zprávy pro jedno místo určení nikdy nesdílejí přenosovou frontu se zprávami pro jiné místo určení.

Změňte atribut správce front **DEFCLXQ** , který řídí výchozí přenosovou frontu klastru, chcete-li vytvořit různé přenosové fronty klastru pro každý odesílací kanál klastru. Více míst určení může sdílet kanál odesílatele klastru, takže musíte naplánovat úplné splnění tohoto cíle v klastrech. Použijte metodu Přidání klastru a přenosové fronty klastru k izolaci přenosu zpráv klastru odesílaného ze správce front brány systematicky do všech front klastru. Výsledkem, jehož cílem je, aby se nesdílely kanál odesílatele klastru s jiným místem určení klastru, není cílem žádného cíle klastru. V důsledku toho žádná zpráva pro místo určení klastru sdílí svou přenosovou frontu klastru se zprávou jiného místa 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 frontu, přidružte ji k odesílacímu kanálu klastru a zastavte a spusťte kanál. Změna nemusí být trvalá. Můžete chvíli izolovat tok zpráv, chcete-li monitorovat přenosovou frontu, a pak se vrátit k použití výchozí přenosové fronty znovu.

Související úlohy

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

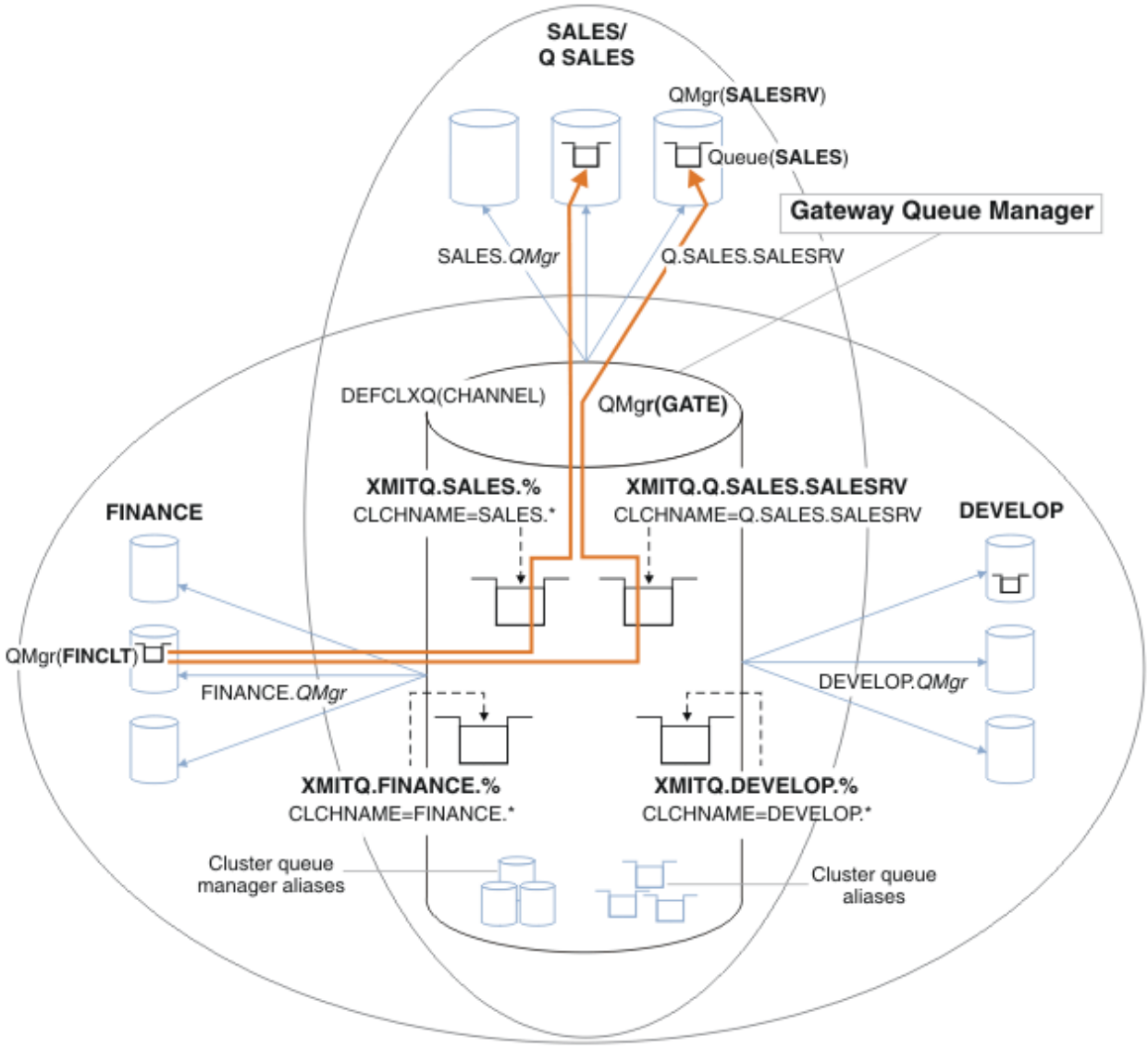
Klastrování: Přepnutí přenosových front klastru
Naplánujte, jak budou uvedeny změny do přenosových front klastru existujícího správce provozní fronty.

Klastrování: Příklad konfigurace více přenosových front klastru
V této úloze použijete tyto kroky k naplánování více přenosových front klastru na tři překrývající se klastry. Požadavky jsou samostatné toky zpráv do jedné fronty klastru, od všech ostatních toků zpráv a pro ukládání 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 49 a dospět k konfiguraci zobrazené v Obrázek 14 na stránce 55. Jedná se o příklad tří překrývajících se klastrů, se správcem front brány, který je konfigurován s oddělenými frontami přenosu klastru. Příkazy MQSC pro definování klastrů jsou popsány v tématu “Vytváření ukázkových klastrů” na stránce 57.

Pro tento příklad existují dva požadavky. Jedna z nich je oddělit tok zpráv od správce front brány k prodejní aplikaci, která protokoluje prodej. Druhým je dotaz na počet zpráv čekajících na odeslání do různých oblastí oddělení v libovolném časovém okamžiku. Klastry `SALES`, `FINANCE`a `DEVELOP` jsou již definovány. Zprávy klastru jsou momentálně přesměrovány z `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.



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

Kroky k úpravě klastrů jsou následující: viz Změny při izolování prodejní fronty v novém klastru a oddělení přenosových front klastru brány pro definice.

Postup

1. První konfigurační krok je na " Vyberte typ výchozí přenosové fronty klastru, která má být použita ".

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

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

   Pro výběr této výchozí hodnoty neexistuje žádný silný důvod, protože záměrem je ručně definovat přenosové fronty klastru. Volba má malou diagnostickou hodnotu. Je-li ruční definice provedena nesprávně a zpráva proteče výchozí přenosovou frontou klastru, zobrazí se při vytváření fronty pro trvalé dynamické přenosové fronty klastru.
2. Druhý krok konfigurace je k " Izolovat jakékoli toky zpráv, které nesmí sdílet přenosovou frontu klastru s jinými toky ".

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

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

Tento příklad vyžaduje přidání správce front SALESRV do nového klastru v rámci prodejního oddělení. Máte-li několik front, které vyžadují izolaci, můžete se rozhodnout pro vytvoření specifického klastru pro frontu SALES . Možnou konvencí pojmenování pro název klastru je pojmenování takových klastrů, `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 tam a kde je to potřeba. 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 k izolování prodejní fronty v novém klastru a oddělené přenosové fronty klastru brány. Souhrn definic změn je následující:

i) Přidejte prostor `Q.SALES` do seznamu názvů klastrů ve správcích front úložiště. Seznam názvů je uveden v parametru **REPOSNL** správce front.

ii) Přidejte `Q.SALES` do seznamu názvů klastrů ve správci front brány. Seznam názvů je ve všech definicích alias fronty klastru a definice alias správce front klastru ve správci front brány označován jako odkaz na seznam alias.

iii) Vytvořte seznam názvů ve správci front SALESRV, pro oba klastry, jehož je členem, a změňte členství klastru ve frontě SALES :

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

Fronta SALES je členem obou klastrů, právě pro přechod. Jakmile je nová konfigurace spuštěna, odeberte frontu produktu SALES z klastru SALES , viz Obrázek 15 na stránce 60.

b) " Vytvořte odesílací kanály klastru a příjemce klastru pro všechny nové klastry, které jste vytvořili podle systematického pojmenování ".

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

ii) Přidejte odesílací kanál klastru `Q.SALES.` *`OtherRepositoryQMgr`* do všech správců front úložiště pro připojení k jinému správci úložiště. Spustit tyto kanály.

iii) Přidejte kanály příjemce klastru `Q.SALES.SALESRV`a `Q.SALES.GATE` do jednoho ze správců front úložiště, kteří jsou spuštění.

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

c) " Definujte přenosovou frontu klastru pro každý izolovaný cíl na 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. Třetí konfigurační krok je na " Vytvořte přenosové fronty klastru, které budou odpovídat požadavkům 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. Eventuálně můžete správce front brány zastavit a spustit.

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
```

Jakmile je přepínač dokončen, odeberte frontu produktu SALES z klastru SALES , viz Obrázek 15 na stránce 60.

Související pojmy

Jak se rozhodnout, jaký typ přenosové fronty klastru použít
Jak si vybrat mezi různými volbami konfigurace přenosové fronty klastru.

Související úlohy

Klastrování: Přepnutí přenosových front klastru
Naplánujte, jak budou uvedeny změny do přenosových front klastru existujícího správce provozní fronty.

Vytváření ukázkových klastrů
Definice a pokyny pro vytvoření vzorového klastru a jejich úpravu k izolaci fronty SALES a oddělené zprávy ve správci front brány.

Informace o této úloze

Úplné příkazy produktu **MQSC** pro vytvoření klastrů FINANCE, SALESa Q.SALES jsou poskytovány v části Definice pro základní klastry, Změny k izolaci prodejní fronty v novém klastru a oddělené přenosové fronty klastru bránya Odeberte prodejní frontu ve správci front SALESRV z klastru prodeje. 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 z názvů správce front v produktu Tabulka 4 na stránce 57.

Tabulka 4. Názvy a čísla portů správce front

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

Tabulka 4. Názvy a čísla portů správce front (pokračování)		
Popis	**Název správce front**	**Číslo portu**
Prodejní server	SALESRV	1419
Komunikační brána	GATE	1420

b) Spustit všechny správce front

Spusťte příkaz: `strmqm` *QmgrName* pro každý z názvů správce front v produktu Tabulka 4 na stránce 57.

c) Vytvořte definice pro každého správce front.

Spusťte příkaz: `runmqsc` *QmgrName* < *filename* , kde jsou soubory uvedeny v části Definice pro základní klastry, a 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 požadavku.
   a) Spuštění programu pro monitorování spouštěčů ve správci front produktu SALESRV

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

   b) Spusťte vzorový program požadavku a odešlete požadavek.

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

      Zpráva požadavku se ozývá zpět a po 15 sekundách, kdy ukázkový program skončí.
3. Vytvořte definice, abyste izolovali frontu SALES v klastru `Q.SALES` a oddělili 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 k izolování prodejní fronty v novém klastru a oddělené přenosové fronty 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 systému Obrázek 15 na stránce 60:

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

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

5. Přepněte kanály na nové přenosové fronty.

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

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

Jak pokračovat dále

1. Znovu spusťte ukázkový program požadavku a ověřte, že nová konfigurace funguje; viz krok “2” na stránce 59
2. Monitorujte zprávy proudící všemi frontami přenosu klastru ve správci front GATE :
   a. Upravte definici každé přenosové fronty klastru tak, aby se monitorování fronty zapnul.

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

   b. Zkontrolujte, zda je monitorování statistiky správce front OFF, aby se minimalizoval výstup, a nastavte interval monitorování na nižší hodnotu, abyste mohli pohodlně provést více testů.

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

   c. Restartujte správce front produktu GATE .
   d. Spusťte vzorový program požadavku několikrát, abyste ověřili, že se stejný počet zpráv proudící přes SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV a SYSTEM.CLUSTER.TRANSMIT.QUEUE. Požaduje tok přes SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV a odpovědi prostřednictvím SYSTEM.CLUSTER.TRANSMIT.QUEUE.

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

   e. Výsledky za několik intervalů 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 druhé. Můžete odvodit, že zprávy požadavku byly umístěny na `SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV`a zprávy odpovědi na `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Klastrování: Přepnutí přenosových front klastru
Naplánujte, jak budou uvedeny změny do přenosových front klastru existujícího správce provozní fronty.

Než začnete

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přechod bude rychlejší. Než budete pokračovat dále, přečtěte si téma Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty z důvodů, proč se pokoušet o vyprázdnění přenosové fronty.

Informace o této úloze

Provedli jste si dva způsoby, jak provést změny v přenosových frontách klastru, které se projeví.

1. Nechat správce front provést změny automaticky. Toto nastavení je výchozí. Správce front přepíná odesílací kanály klastru s nevyřízenými změnami přenosové fronty při příštím spuštění kanálu odesílatele klastru.
2. Proveďte změny ručně. Změny kanálu odesílatele klastru můžete změnit, až bude zastaven. Před spuštěním kanálu odesílatele klastru můžete přepnout z jedné přenosové fronty klastru do jiné.

Jaké faktory byste měli vzít v úvahu při rozhodování o tom, které z těchto dvou možností vybrat, a jak se řídit přepínač?

Procedura

- Volba 1: Nechat správce front provést změny automaticky; viz “Přepínání aktivních odesílacích kanálů klastru na jinou sadu front-přenosových front” na stránce 63.

  Vyberte tuto volbu, chcete-li, aby se pro vás správce front přepínal.

  Alternativním způsobem popisu této volby je říci, že správce front přepne odesílací kanál klastru bez vynucení zastavení kanálu. Máte možnost donutit kanál zastavit a pak spustit kanál, aby se přepnutí stalo dříve. Přepínač se spustí, když se kanál spustí a spustí se, zatímco je spuštěn kanál, což se liší od volby 2. Ve volbě 2 se přepínač provádí, když je kanál zastaven.

  Vyberete-li tuto volbu tím, že necháte přepínač automaticky, spustí se proces přepínání při spuštění kanálu odesílatele klastru. Není-li kanál zastaven, bude spuštěn poté, co se stane neaktivní, pokud bude existovat nějaká zpráva ke zpracování. Je-li kanál zastaven, spusťte jej pomocí příkazu `START CHANNEL` .
  Proces přepnutí se dokončí, jakmile v přenosové frontě kanálu, který kanál obsluhuje, nezůstalo žádné zprávy, které byly ponechány pro odesílací kanál klastru. Jakmile je tomu tak, jsou nově příchozí zprávy pro odesílací kanál klastru ukládány přímo do nové přenosové fronty. Do té doby jsou zprávy ukládány do staré přenosové fronty a proces přepínání přenáší zprávy ze staré přenosové fronty do nové přenosové fronty. Odesílací kanál klastru předává zprávy z nové přenosové fronty klastru během celého procesu přepínání.

Jakmile proces přepínače skončí, závisí na stavu systému. Provádíte-li změny v okně údržby, předem vyhodnoťte, zda bude proces přepínání dokončen včas. Zda bude dokončeno v čase záleží na tom, zda počet zpráv čekajících na přenos ze staré přenosové fronty dosáhne nuly.

Výhoda první metody je automatická. Nevýhodou je, že pokud čas pro provedení změn konfigurace je omezen na okno údržby, musíte mít jistotu, že můžete systém řídit, abyste dokončili proces přepnutí uvnitř okna údržby. Pokud si nemůžete být jisti, volba 2 může být lepší volbou.

- Volba 2: Proveďte změny ručně; viz “Přepnutí zastaveného odesílacího kanálu klastru do jiné přenosové fronty klastru” na stránce 64.

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

  Alternativní popis této volby znamená, že jste přepnuli odesílací kanál klastru, zatímco kanál odesílatele klastru je zastaven.

  Vyberete-li tuto volbu, máte úplnou kontrolu nad tím, kdy dojde k přepnutí.
  Můžete si být jisti o dokončení procesu přepínání v pevně stanoveném čase, v rámci okna údržby. Doba, kterou přepnutí zabere, závisí na tom, kolik zpráv se má přenést z jedné přenosové fronty do druhé. Pokud se zprávy dostaví, může chvíli trvat, než bude proces přenášet všechny zprávy.
  Máte možnost přepnout kanál bez přenosu zpráv ze staré přenosové fronty. Přepínač je "instant".
  Když restartujete odesílací kanál klastru, začne zpracovávat zprávy v přenosové frontě, kterou jste k ní nově přiřadili.

  Výhodou druhé metody je, že máte kontrolu nad procesem přepínání. Nevýhodou je, že musíte identifikovat kanály odesílatele klastru, které mají být přepnuty, spustit potřebné příkazy a vyřešit všechny nejisté kanály, které by mohly bránit zastavování kanálu odesílatele klastru.

Související pojmy

Jak se rozhodnout, jaký typ přenosové fronty klastru použít
Jak si vybrat mezi různými volbami konfigurace přenosové fronty klastru.

Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje

Související úlohy

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

Přepínání aktivních odesílacích kanálů klastru na jinou sadu front-přenosových front
Tato úloha vám poskytuje tři volby pro přepínání aktivních odesílacích kanálů klastru. Jednou z možností je nechat správce front přepnout přepínač automaticky, což nemá vliv na běžící aplikace. Další volby slouží k ručnímu zastavení a spuštění kanálů nebo k restartování správce front.

Než začnete

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

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přechod bude rychlejší. Než budete pokračovat dále, přečtěte si téma Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty z důvodů, proč se pokoušet o vyprázdnění přenosové fronty.

Informace o této úloze

Použijte kroky v úloze jako základ pro práci vlastního plánu pro provedení změn konfigurace přenosové fronty klastru.

Postup

1. Volitelné: Zaznamenat aktuální stav kanálu

   Vytvořte záznam o stavu aktuálních a uložených kanálů, které obsluhují přenosové fronty klastru. Následující příkazy zobrazují stav vztahující se k přenosovým frontám systémového klastru. Přidejte své vlastní příkazy, abyste zobrazili stav přidružený k frontám přenosu klastru, které jste definovali. Použijte konvenci, jako například XMITQ. *ChannelName*, abyste pojmenovali přenosové fronty klastru, které definujete, aby bylo snadné zobrazit stav kanálu pro přenosové fronty.

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

2. Přepínat přenosové fronty.

   - Nedělejte nic. Správce front přepíná odesílací kanály klastru, když se restartují po zastavení nebo nečinnosti.

     Tuto volbu vyberte v případě, že nemáte žádná pravidla nebo problémy týkající se změny konfigurace správce front. Spuštěné aplikace nejsou změnami ovlivněny.
   - Restartujte správce front. Všechny odesílací kanály klastru jsou zastavené a restartovány automaticky na vyžádání.

     Vyberte tuto volbu, chcete-li okamžitě zahájit všechny změny. Spuštěné aplikace jsou správcem front přerušeny, jakmile se ukončí a znovu spustí.
   - Zastavte jednotlivé odesílací kanály klastru a restartujte je.

     Vyberte tuto volbu, chcete-li okamžitě změnit několik kanálů. Spuštění aplikací se setká s krátkou prodlevou při přenosu zpráv mezi zastavením a opětovným spuštěním kanálu zpráv. Odesílací kanál klastru zůstává spuštěn, s výjimkou případů, kdy jste jej zastavili. Během zpráv procesu přepnutí se doručují do staré přenosové fronty, přenáší se do nové přenosové fronty procesem přepnutí a přeposláno z nové přenosové fronty kanálem odesílatele klastru.
3. Volitelné: Monitorování kanálů při přepnutí

   Zobrazuje stav kanálu a hloubku přenosové fronty během přepnutí. Následující příklad zobrazuje stav přenosových front 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: Monitorování zpráv AMQ7341 `Přenosová fronta pro kanál` *ChannelName* `byla přepnuta z fronty` *QueueName* `do` *QueueName* , která jsou zapsána do protokolu chyb správce front.

Přepnutí zastaveného odesílacího kanálu klastru do jiné přenosové fronty klastru
Rozhodnete-li se provést změny ručně, provedete změny v kanálu odesílatele klastru při jeho zastavení a přepnete jej z jedné přenosové fronty klastru do jiné před spuštěním kanálu odesílatele klastru.

Než začnete

Můžete provést některé změny konfigurace a nyní je chcete zefektivníte bez toho, aby byly ovlivněny kanály odesílatele klastru, které jsou ovlivněny. Případně provedete změny konfigurace, které potřebujete jako jeden z kroků v úloze.

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přechod bude rychlejší. Než budete pokračovat dále, přečtěte si téma Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty z důvodů, proč se pokoušet o vyprázdnění přenosové fronty.

Informace o této úloze

Tato úloha přepíná přenosové fronty obsluhované zastavené nebo neaktivní odesílací kanály klastru. Tuto úlohu můžete provést, protože kanál odesílatele klastru je zastaven a vy chcete ihned přepnout jeho přenosovou frontu. Například z nějakého důvodu se nespouští odesílací kanál klastru, nebo má nějaký jiný konfigurační problém. Chcete-li tento problém vyřešit, rozhodnete se vytvořit odesílací kanál klastru a asociovat přenosovou frontu pro starý kanál odesílatele klastru s použitím nového odesílacího kanálu klastru, který jste definovali.

Pravděpodobnější scénář je, že chcete řídit, je-li provedena změna konfigurace přenosových front klastru. Chcete-li plně řídit překonfiguraci, zastavte kanály, změňte konfiguraci a poté přepněte přenosové fronty.

Postup

1. Zastavte kanály, které chcete přepnout.
   a) Zastavte všechny spuštěné nebo neaktivní kanály, které chcete přepnout. Zastavení neaktivního kanálu odesílatele klastru zabrání tomu, aby se spouštěli při provádění změn konfigurace.

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

2. Volitelné: Proveďte změny konfigurace.

   Například viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 54.
3. Přepněte odesílací kanály klastru na nové přenosové fronty klastru.

   Multi V systému Multiplatformszadejte následující příkaz:

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

   z/OS V systému z/OSpoužijte k přepnutí zpráv nebo monitorování toho, co se děje, funkci SWITCH příkazu CSQUTIL. Použijte následující příkaz.

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

   Další informace viz Funkce SWITCH.

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

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

   Vzhledem k tomu, že kanál odesílatele klastru je zastaven, budou zprávy navazovat na novou přenosovou frontu. Porovnejte zastavený kanál odesílatele klastru, na krok “2” na stránce 64 v příručce “Přepínání aktivních odesílacích kanálů klastru na jinou sadu front-přenosových front” na stránce 63. V tomto kroku je kanál odesílatele klastru spuštěn, takže zprávy nemusí být nutně sestaveny v nové přenosové frontě.
4. Volitelné: Monitorování kanálů při přepnutí

   V okně s jiným příkazovým řádkem se zobrazí hloubka přenosové fronty během přepnutí. Následující příklad zobrazuje stav přenosových front systémového klastru.

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

5. Volitelné: Monitorování zpráv AMQ7341 `Přenosová fronta pro kanál ChannelName byla přepnuta z fronty QueueName do QueueName` , která jsou zapsána do protokolu chyb správce front.
6. Restartujte odesílací kanály klastru, které jste zastavili.

Kanály se nespustí automaticky, jakmile je zastavíte, umístíte je do stavu STOPPED .

```
START CHANNEL(ChannelName)
```

Související odkazy
runswchl
Vyřešit kanál
Ukončit kanál

Klastrování: migrace a úprava doporučených postupů
Toto téma obsahuje pokyny pro plánování a administraci klastrů IBM MQ . Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

1. “Přesun objektů v klastru” na stránce 66 (Nejlepší postupy pro přesouvání objektů v rámci klastru bez instalace oprav FixPack nebo nových verzí produktu IBM MQ).
2. “Upgrade a údržba instalací” na stránce 67 (Nejlepší postupy pro udržení funkční architektury klastrů při použití údržby nebo přechodů na vyšší verzi a testování nové architektury).

Přesun objektů v klastru

Aplikace a jejich fronty

Je-li třeba přesunout instanci fronty, jejímž hostitelem je jeden správce front, pracovat s parametry vyrovnávání pracovní zátěže, můžete pracovat s parametry vyrovnávání pracovní zátěže, abyste zajistili hladký přechod.

Vytvořte instanci fronty, kde má být nově hostována, ale použijte nastavení vyrovnávání pracovní zátěže klastru pro pokračování odesílání zpráv do původní instance, dokud nebude vaše aplikace připravena k přepnutí. Toho lze dosáhnout následujícím způsobem:

1. Nastavte vlastnost **CLWLRANK** existující fronty na vysokou hodnotu, například pět.
2. Vytvořte novou instanci fronty a nastavte její vlastnost **CLWLRANK** na hodnotu nula.
3. Dokončete další konfiguraci nového systému, například implementujte a spusťte aplikace spotřebovávající aplikaci proti nové instanci fronty.
4. Nastavte vlastnost **CLWLRANK** nové instance fronty na vyšší, než je původní instance, například devět.
5. Nechejte původní instanci fronty zpracovat všechny zprávy zařazené do fronty v systému a pak odstraňte frontu.

Přesun celých správců front

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

- DNS, je-li použit správně, může pomoci zjednodušit proces. Informace o použití DNS nastavením atributu kanálu Název připojení (CONNAME) naleznete v tématu ALTER CHANNEL.
- Při přesouvání úplného úložiště se ujistěte, že máte alespoň jedno další úplné úložiště, které běží hladce (bez problémů se stavem kanálu) před provedením změn.
- Pomocí příkazu SUSPEND QMGR pozastavte správce front tak, aby nedošlo k hromadným přenosům.
- Upravte adresu IP počítače. Pokud definice kanálu CLUSRCVR používá adresu IP v poli CONNAME, upravte tento záznam adresy IP. Je možné, že je třeba vyprázdnit mezipaměť DNS, aby bylo zajištěno, že jsou k dispozici aktualizace všude.
- Když se správce front znovu připojí k úplným úložištím, automatické definice kanálu se automaticky vyřeší samy.
- Pokud správce front hostil úplné úložiště a došlo ke změně adresy IP, je důležité zajistit, aby byly části přepnuty co nejdříve, aby byly ručně definované kanály CLUSSDR přidány do nového umístění. Dokud nebude tento přepínač proveden, mohou být tito správci front schopni kontaktovat pouze

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

- Obnovte správce front pomocí příkazu RESUME QMGR .

Je-li třeba správce front přesunout na nového hostitele, je možné zkopírovat data správce front a obnovit je ze zálohy. Tento proces se však nedoporučuje, pokud neexistují jiné možnosti. Může být lepší vytvořit správce front v novém počítači a replikovat fronty a aplikace, jak je popsáno v předchozí sekci. Tato situace poskytuje plynulý mechanismus rolování/odvolání.

Pokud jste odhodláni přesunout kompletního správce front s použitím zálohování, postupujte podle následujících doporučených postupů:

- Zacházet s celým procesem jako s obnovou správce front ze zálohy a aplikovat všechny procesy, které byste obvykle používali pro obnovu systému, jak je to vhodné pro prostředí operačního systému.
- Použijte příkaz **REFRESH CLUSTER** po migraci k vyřazení všech lokálně zadržovaných informací o klastru (včetně všech automaticky definovaných kanálů, které jsou nejisté) a vynuťte 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 je popsáno výše v tomto tématu) se nikdy nezpracují dva různé správce front jako ve skutečnosti stejné. Zejména nepojmenujte nového správce front se stejným názvem správce front a adresou IP. Pokus o 'zrušení' náhradního správce front je častou příčinou problémů v klastrech produktu IBM MQ . Mezipaměť očekává přijetí aktualizací včetně atributu **QMID** a stav může být poškozen.

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

Upgrade a údržba instalací

Vyhněte se takzvanému scénáři velkých bang (například zastavení všech aktivit klastrů a správců front, použití všech upgradů a údržby pro všechny správce front, pak spuštění všeho ve stejnou dobu). Klastry jsou navrženy tak, aby stále pracovaly s více verzemi koexistujících správců front, takže je doporučen dobře naplánovaný přístup pro údržbu po etapách.

Připravte si záložní plán:

- Zbali jste se zálohy?
- Vyvarovat se použití nových funkcí klastru okamžitě: Počkejte, až budete mít jistotu, že všichni správci front jsou upgradováni na novou úroveň a že jste si jisti, že se z nich nechystáte odvolat žádné. Použití nové funkce klastru v klastru, v němž jsou někteří správci front stále na nižší úrovni, může vést k nedefinovanému chování. For example, in the move to IBM WebSphere MQ 7.1 from IBM WebSphere MQ 6.0, if a queue manager defines a cluster topic, IBM WebSphere MQ 6.0 queue managers will not understand the definition or be able to publish on this topic.

Nejprve proveďte migraci úplných úložišť. I když mohou předat informace, které nerozumí, nemohou ji trvale uchovají, takže to není doporučovaný přístup, pokud to není absolutně nezbytné. Další informace naleznete v tématu Migrace klastru správce front.

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER
Příkaz **REFRESH CLUSTER** se používá k zahození všech lokálně uložených informací o klastru a znovusestavení těchto informací z úplných úložišť v klastru. Tento příkaz byste neměli používat, kromě výjimečných okolností. Pokud ji potřebujete použít, musíte zvážit, jak ji budete používat. Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

Spustit pouze příkaz REFRESH CLUSTER, pokud je to opravdu nutné provést.

Technologie klastrů produktu IBM MQ zajišťuje, že jakákoli změna konfigurace klastru, jako je změna na klastrovanou frontu, se automaticky stane známým členovi klastru, který potřebuje informace znát. Není třeba učinit další správní kroky k dosažení tohoto šíření informací.

Pokud se tyto informace nedostanete do správců front v klastru, kde je to vyžadováno, například klastrovaná fronta není známa jiným správcem front v klastru, když se aplikace pokusí ji otevřít poprvé, znamená to, že se jedná o problém v infrastruktuře klastru. Například je možné, že kanál nelze spustit mezi správcem front a úplným správcem front úložiště. Proto musí být prošetřena každá situace, v níž jsou zjištěny nesrovnalosti. Je-li to možné, vyřešte situaci bez použití příkazu **REFRESH CLUSTER** .

Za výjimečných okolností, které jsou zdokumentovány jinde v této dokumentaci produktu, nebo pokud požadujete podporu produktu IBM , můžete použít příkaz **REFRESH CLUSTER** k zahození všech lokálně uchovávané informace o klastru a znovusestavení těchto informací z úplných úložišť v klastru.

Aktualizace ve velkém klastru může ovlivnit výkon a dostupnost klastru.

Použití příkazu **REFRESH CLUSTER** může být pro klastr rušivé, zatímco probíhá jeho zpracování, například při vytváření náhlého zvýšení práce pro úplná úložiště při zpracování opětovného šíření prostředků klastru správce front. Pokud obnovujete ve velkém klastru (tj. mnoha stovkám správců front), měli byste se vyhnout použití příkazu v každodenní práci, pokud možno a použít alternativní metody k nápravě konkrétních nekonzistencí. Pokud například fronta klastru není správně propagována v rámci klastru, bude počáteční technika pro aktualizaci definice klastrované fronty, jako je například změna popisu, znovu šířena konfigurací fronty v rámci klastru. Tento proces může pomoci identifikovat problém a potenciálně vyřešit dočasnou nekonzistenci.

Pokud nelze použít alternativní metody a musíte spustit prostor **REFRESH CLUSTER** ve velkém klastru, měli byste to provést ve vypnutém čase nebo v průběhu okna údržby, abyste se vyhnuli vlivu na pracovní zátěže uživatelů. Měli byste se také vyhnout obnově velkého klastru v jedné dávce a místo toho, abyste aktivitu fázovali, jak je vysvětleno v tématu “Vyvarovat se problémů s výkonem a dostupností, když objekty klastru odesílají automatické aktualizace” na stránce 68.

Vyvarovat se problémů s výkonem a dostupností, když objekty klastru odesílají automatické aktualizace

Po definování nového objektu klastru ve správci front je aktualizace tohoto objektu generována každých 27 dnů od definice času a odešle se do každého úplného úložiště v klastru a dále do všech dalších zainteresovaných správců front. Když vydáte příkaz **REFRESH CLUSTER** správci front, resetujete hodiny pro tuto automatickou aktualizaci na všech objektech definovaných lokálně v uvedeném klastru.

Pokud obnovíte velký klastr (to znamená mnoho stovek správců front) v jedné dávce nebo za jiných okolností, jako je opětovné vytvoření systému ze zálohy konfigurace, po 27 dnech všichni tito správci front znovu ohlásí všechny své definice objektů do úplných úložišť současně. To může znovu způsobit, že systém se výrazně zpomalí, nebo se dokonce stane nedostupným, dokud nebudou dokončeny všechny aktualizace. Proto, když budete muset obnovit nebo znovu vytvořit více správců front ve velkém klastru, měli byste aktivitu fázovat přes několik hodin nebo několik dní, aby následné automatické aktualizace neovlivňovaly výkon systému.

Fronta historie systémového klastru

Je-li provedeno **REFRESH CLUSTER** , správce front pořídí snímek stavu klastru před obnovou a uloží jej na `SYSTEM.CLUSTER.HISTORY.QUEUE` (SCHQ), pokud je definován ve správci front. Tento snímek je určen pouze pro servisní účely IBM , v případě pozdějších problémů se systémem.

SCHQ je standardně definován u distribuovaných správců front při spuštění. Pro migraci produktu z/OS musí být položka SCHQ ručně definována.

Platnost zpráv o SCHQ vyprší za tři měsíce.

Související pojmy

“Aspekty REFRESH CLUSTER pro klastry publikování/odběru” na stránce 102
Vydáním příkazu **REFRESH CLUSTER** se ve správci front dočasně zruší lokální zadržení informací o klastru, včetně všech témat klastru a jejich přidružených proxy odběrů.

Problémy aplikace zaznamenané při spuštění REFRESH CLUSTER

Související odkazy

Popis příkazů MQSC: REFRESH CLUSTER

Klastrování: Dostupnost, víceinstanční instalace a zotavení z havárie
Toto téma obsahuje pokyny pro plánování a administraci klastrů IBM MQ . Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

IBM MQ Klastrování samo o sobě není řešením vysoké dostupnosti, ale za určitých okolností může být použito ke zlepšení dostupnosti služeb pomocí produktu IBM MQ, například tím, že má více instancí fronty v různých správcích front. Tento oddíl poskytuje pokyny k zajištění co nejvyšší dostupnosti infrastruktury produktu IBM MQ , aby bylo možné ji 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
Důvodem pro obvyklé doporučení k zachování dvou úplných úložišť je to, že ztráta jednoho z nich není kritická pro plynulé spouštění klastru. I když se obě stanou nedostupnými, existuje 60denní doba odkladu pro existující znalosti, které se nacházejí v částečných úložištích, ačkoli v této události nejsou k dispozici nové nebo dříve nedostupné prostředky (fronty pro příklad).

Použití klastrů ke zlepšení dostupnosti aplikací
Klastr může pomoci při návrhu vysoce dostupných aplikací (například serverová aplikace typu požadavek/odezva), a to pomocí více instancí fronty a aplikace. Je-li to nutné, atributy priority mohou upřednostňovat aplikaci 'live', pokud například správce front nebo kanál nejsou k dispozici. To je výkonné pro rychlý přechod na pokračování zpracování nových zpráv, když se vyskytne problém.

Zprávy, které byly doručeny určitému správci front v klastru, jsou však drženy pouze v této instanci fronty a nejsou k dispozici pro zpracování, dokud nebude tento správce front obnoven. Z tohoto důvodu můžete pro skutečnou dostupnost dat zvážit použití jiných technologií, jako jsou správci front s více instancemi.

Správci front s více instancemi
Software High Availability (multi-instance) je vestavěná nabídka pro zachování dostupnosti stávajících zpráv. Další informace naleznete v tématu Použití produktu IBM MQ s konfiguracemi vysoké dostupnosti, Vytvoření správce front s více instancemia následující sekce. Jakýkoli správce front v klastru může být prostřednictvím této techniky vysoce dostupný, pokud jsou všichni správci front v klastru spuštění alespoň IBM WebSphere MQ 7.0.1. Jsou-li všichni správci front v klastru na předchozí úrovni, mohou ztratit konektivitu s správci front pro více instancí, pokud dojde k selhání na sekundární adresu IP.

Jak již bylo uvedeno výše v tomto tématu, pokud jsou konfigurována dvě úplná úložiště, jsou téměř svým charakterem vysoce dostupní. Je-li třeba, lze pro úplná úložiště použít software IBM MQ High Availability/multi-instance správce front. Neexistuje žádný silný důvod používat tyto metody, a ve skutečnosti pro dočasné výpadky mohou tyto metody způsobit další výkonnostní náklady během překonání selhání. Použití softwaru HA namísto spuštění dvou úplných úložišť je nevhodné, protože v případě výskytu jednoho výpadku kanálu by například nemuselo dojít k selhání, ale může opustit částečná úložiště, která nemohou dotazy na prostředky klastru dotazovat.

Zotavení z havárie
Zotavení z havárie, například zotavení z toho, kdy jsou disky ukládající data správce front poškozeny, je obtížné dobře; IBM MQ může pomoci, ale nemůže to dělat automaticky. Jediná volba 'true' pro zotavení z havárie v produktu IBM MQ (kromě jakéhokoliv operačního systému nebo jiných základních technologií replikace) je obnova ze zálohy. V těchto situacích je třeba zvážit několik specifických aspektů klastru:

- Dávejte pozor při testování scénářů zotavení z havárie. Pokud například testujete operaci se správci front zálohování, buďte opatrní při jejich uvedení do stavu online ve stejné síti, protože je možné náhodně připojit aktivní klastr a začít 'kradení' zpráv hostováním stejných pojmenovaných front jako v aktivních správcích front klastru.
- Testování zotavení z havárie nesmí kolidovat se spuštěným aktivním klastrem. Techniky zabraňování interferenci zahrnují:
  - Dokončete oddělování sítě nebo oddělení na úrovni brány firewall.
  - z/OS Nespouští se inicializace kanálu nebo adresní prostor z/OS **chinit** .
  - Do systému zotavení z havárie se nevydává živý certifikát TLS, dokud nedojde ke skutečnému scénáři zotavení z havárie.
- Když obnovujete zálohu správce front v klastru, je možné, že záloha nebude synchronizována se zbytkem klastru. Příkaz **REFRESH CLUSTER** může vyřešit aktualizace a synchronizovat s klastrem, ale příkaz **REFRESH CLUSTER** se musí použít jako poslední možnost. Viz “Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 67. Chcete-li zjistit, zda byl před použitím příkazu použit jednoduchý krok, prostudujte si všechny interní dokumentaci procesu a dokumentaci produktu IBM MQ .
- Pokud jde o jakékoli zotavení, aplikace se musí vypořádat s přehráním a ztrátou dat. Je třeba se rozhodnout, zda vymazat fronty do známého stavu, nebo pokud existuje dostatek informací pro správu přehraných informací.

Plánování distribuované sítě pro publikování/odběr

Můžete vytvořit síť správců front, ve kterých odběry vytvořené v jednom správci front obdrží 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, četnost změn, dostupnost a rozšiřitelnost.

Než začnete

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

Informace o této úloze

Pro síť typu publikování/odběr existují tři základní topologie:

- Přímý směrovaný klastr
- Klastr routed hostitelem tématu
- Hierarchie

U prvních dvou topologií je počátečním bodem konfigurace klastru produktu IBM MQ . Třetí topologie může být vytvořena s klastrem nebo bez něj. Informace o plánování základní sítě správců front naleznete v příručce“Plánování vašich distribuovaných front a klastrů” na stránce 19.

Přímý směrovaný klastr je nejjednodušší topologie, která se má nakonfigurovat, když je již klastr přítomen. Jakékoli téma, které definujete v libovolném správci front, je automaticky zpřístupněno v každém správci front v klastru a publikace jsou směrovány přímo z libovolného správce front, kde se připojuje publikační aplikace, ke každému správci front, v němž existují odpovídající odběry. Tato jednoduchost konfigurace spoléhá na to, že produkt IBM MQ udržuje vysokou úroveň sdílení informací a propojitelnosti mezi každým správcem front v klastru. Pro malé a jednoduché sítě (tj. malý počet správců front a poměrně statická sada vydavatelů a odběratelů) je to přijatelné. Avšak při použití ve větších nebo dynamičtějších prostředích může být režie příliš prohibiční. Viz“Přímé směrování v klastrech publikování/odběru” na stránce 75.

Klastr routed routed tématu poskytuje stejný užitek jako přímo směrovaný klastr, a to tak, že všechny téma, které definujete ve správci front v klastru, je automaticky dostupné ve všech správcích front v klastru. Klastry se směrováním hostitele témat však vyžadují, abyste si pečlivě vybrali správce front, kteří jsou hostiteli jednotlivých témat, protože všechny informace a publikace pro dané téma procházejí

správci front hostitele tématu. To znamená, že systém nemusí udržovat kanály a informační toky mezi všemi správci front. Znamená to však také to, že publikace již nemusí být zasílány přímo odběratelům, ale mohou být směrovány prostřednictvím správce front hostitele tématu. Z těchto důvodů může být do systému vložena další zátěž, zejména na správce front, který je hostitelem témat, proto je třeba pečlivě naplánovat topologii. Tato topologie je zvláště efektivní pro sítě, které obsahují mnoho správců front, nebo které jsou hostiteli dynamické sady vydavatelů a odběratelů (tj. vydavatelé nebo odběratelé, kteří jsou často přidáni nebo odebírány). Další hostitelé témat lze definovat, chcete-li zlepšit dostupnost přenosových cest a horizontálně rozšiřovat pracovní zátěž publikování. Viz“Směrování hostitele témat v klastrech publikování/odběru” na stránce 80.

Hierarchie vyžaduje, aby byla nastavena většina ruční konfigurace a která je nejtvrdší topologie, která se má upravit. Vztah mezi každým správcem front v hierarchii a jeho přímými vztahy musíte nakonfigurovat ručně. Po konfiguraci vztahů budou publikace (jako pro předchozí dvě topologie) směrovány na odběry v jiných správcích front v hierarchii. Publikace jsou směrovány pomocí relací hierarchie. To umožňuje nakonfigurovat velmi specifické topologie, aby vyhovovaly různým požadavkům, ale může také vyústit v publikování vyžadující mnoho "přechodů" zprostředkujících správci front k dosažení odběrů. Pro publikování existuje vždy pouze jedna trasa v rámci hierarchie, takže dostupnost každého správce front je kritická. Hierarchie jsou obvykle výhodnější pouze v případě, kdy nelze konfigurovat jediný klastr; například při rozmírování více organizací. Viz“Směrování v hierarchiích publikování/odběru” na stránce 103.

V případě potřeby mohou být výše uvedené tři topologie kombinovány s cílem vyřešit specifické topografické požadavky. Příklad naleznete v tématu Sloučení prostorů tématu u více klastrů.

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

- Jak velká bude vaše síť?
- Kolik manuální kontroly potřebujete přes jeho konfiguraci?
- Jak dynamický bude systém, a to jak z hlediska témat a odběrů, tak i 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 by vaše síť měla být.
  a) Odhadněte, kolik témat potřebujete.
  b) Odhadněte počet vydavatelů a odběratelů, které očekáváte, že budete mít.
  c) Odhadněte, kolik správců front bude zahrnuto do aktivit publikování/odběru.

     Viz také“Klastrování publikování/odběru: Nejlepší postupy” na stránce 89, a to zejména následující sekce:

     – Jak upravit velikost systému
     – Důvody k omezení počtu správců front klastru zahrnutých do aktivity publikování/odběru
     – Jak rozhodnout, která témata do klastru

  Pokud bude vaše síť mít mnoho správců front a pracovat s mnoha vydavateli a odběrateli, pravděpodobně budete muset použít klastr se směrováním hostitele tématu nebo hierarchii. Přímo směrované klastry vyžadují téměř žádnou manuální konfiguraci a mohou být dobrým řešením pro malé nebo statické sítě.
- Zvažte, kolik ručních ovládacích prvků budete potřebovat k tomu, který správce front je hostitelem každého tématu, vydavatele nebo odběratele.
  a) Zvažte, zda některé z vašich správců front jsou méně schopné než jiné.
  b) Zvažte, zda jsou komunikační odkazy na některé z vašich správců front křehčí než u ostatních.
  c) Identifikujte případy, ve kterých očekáváte, že téma bude mít mnoho publikací a málo odběratelů.

d) Identifikujte případy, ve kterých očekáváte, že téma bude mít mnoho odběratelů a málo publikací.

Ve všech topologiích jsou publikace dodávány do odběrů u jiných správců front. V klastru s přímým směrováním se tyto publikace nacházejí v nejkratší cestě k odběrům. V klastru se směrovaným hostitelem témat nebo hierarchii můžete řídit trasu, která bude provádět publikování. Pokud se vaši správci front liší od svých schopností nebo mají různé úrovně dostupnosti a konektivity, pravděpodobně budete chtít přiřadit specifické pracovní zátěže specifickým správcům front. To lze provést buď pomocí klastru routed hostitelem tématu, nebo pomocí hierarchie.

Ve všech topologiích společně umisťování publikujících aplikací do stejného správce front jako odběrů, pokud je to možné, minimalizuje režii a maximalizuje výkon. V případě klastrů se směrováním hostitele zvažte vložení vydavatelů nebo odběratelů na správce front, kteří jsou hostitelem daného tématu. Tím dojde k odebrání všech dalších "přechodů" mezi správci front za účelem předání publikování odběrateli. Tento přístup je zvláště účinný v případech, kdy téma má mnoho vydavatelů a málo odběratelů, nebo mnoho vydavatelů a málo vydavatelů. Viz například téma Směrování hostitele tématu pomocí centralizovaných vydavatelů nebo odběratelů.

Viz také“Klastrování publikování/odběru: Nejlepší postupy” na stránce 89, a to zejména následující sekce:

– Jak rozhodnout, která témata do klastru
– Vydavatel a umístění odběru

- Zvažte, jak bude dynamická aktivita sítě.
  a) Odhadněte, jak často budou odběratelé přidáni a odebrání z různých témat.

  Kdykoli je přidán nebo odebrán odběr ze správce front a je to první nebo poslední odběr pro daný řetězec tématu, jsou tyto informace sděleny ostatním správcům front v topologii. V přímém směrovém klastru a v hierarchii se informace o odběru šíří do každého správce front v topologii bez ohledu na to, zda mají vydavatele na dané téma. Pokud se topologie skládá z mnoha správců front, může to být významná výkonnostní režie. V klastru se směrováním hostitelů témat jsou tyto informace šířeny pouze do těch správců front, kteří jsou hostiteli klastrového tématu, které je mapováeno na řetězec tématu odběru.

  Viz také část Subscription change and dynamic topic strings v příručce“Klastrování publikování/odběru: Nejlepší postupy” na stránce 89.

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

  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, přičemž je třeba dbát na to, aby při změně správců front na vyšší úrovni v hierarchii. Správci front v hierarchii obvykle používají také ručně konfigurovaná připojení kanálů. Tato připojení je třeba udržovat, přidávat a odebírat kanály jako správce front, a odebírat je z hierarchie.

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

- Zvažte požadavky na rozšiřitelnost a požadavky na rozšiřitelnost v rámci své trasy.
  a) Rozhodněte se, zda potřebujete mít vždy dostupnou trasu ze správce front publikování do odběratelského správce front, a to i v případě, že je správce front nedostupný.
  b) Zvažte, jak přizpůsobitelná je síť, která má být. Rozhodněte se, zda je úroveň provozu publikování příliš vysoká, než aby byla směrována prostřednictvím jednoho správce front nebo kanálu, a zda má být tato úroveň provozu publikování zpracována jedinou větví tématu, nebo může být rozložena mezi více větví témat.
  c) Zvažte, zda je třeba zachovat pořadí zpráv.

  Vzhledem k tomu, že přímý směrovaný klastr odesílá zprávy přímo ze správců front do odběratelských správců front, není třeba brát v úvahu dostupnost zprostředkujících správců front v rámci trasy.

Podobně změna měřítka pro zprostředkující správce front není zvažovanou. Avšak, jak bylo uvedeno dříve, režie automatického udržování kanálů a informačních toků mezi všemi správci front v klastru může výrazně ovlivnit výkon, zejména ve velkém nebo dynamickém prostředí.

Klastr routed routed může být vyladěn pro jednotlivá témata. Můžete zajistit, aby každá větev stromu témat, která má značnou pracovní zátěž publikování, byla definována v odlišném správci front a aby každý správce front byl dostatečně výkonný a aby byl k dispozici pro očekávanou pracovní zátěž pro příslušnou větev stromu témat. Můžete také zlepšit dostupnost a horizontálnější škálování tak, že definujete každé téma ve více správcích front. To umožňuje systému směrovat okolo nedostupných správců front hostitele tématu a vyrovnávat pracovní zátěž po publikování v rámci pracovní zátěže. Když však definujete dané téma ve více správcích front, představíte také následující omezení:

- V rámci publikací ztratíte pořadí zpráv.
- Zachované publikace nelze používat. Viz"Aspekty návrhu pro zachovaná publikování v klastrech publikování/odběru" na stránce 101.

Prostřednictvím více tras nelze konfigurovat vysokou dostupnost nebo rozšiřitelnost směrování v rámci hierarchie.

Viz také část Publication traffic v příručce"Klastrování publikování/odběru: Nejlepší postupy" na stránce 89.

- Na základě těchto výpočtů můžete použít poskytnuté odkazy, které vám pomohou rozhodnout se, zda použít klastr se směrováním hostitele témat, přímo směrovaný klastr, hierarchii nebo kombinaci těchto topologií.

Jak pokračovat dále

Nyní jste připraveni konfigurovat síť distribuovaného publikování/odběru.

Související úlohy

Konfigurace klastru správce front

Konfigurace distribuovaných front

Konfigurace klastru publikování/odběru

Připojení správce front k hierarchii publikování a odběru

Návrh klastrů publikování a odběru

Existují dvě základní topologie klastru pro publikování/odběr: *přímé směrování* a *směrování hostitele témat*. Každý z nich má jiné výhody. Při navrhování klastru pro publikování/odběr zvolte topologii, která nejlépe odpovídá očekávaným požadavkům na síť.

Přehled dvou klastrů publikování/odběru klastru naleznete v tématu Klastry publikování/odběru. Informace o tom, jak lze vyhodnotit požadavky na síť, naleznete v části "Plánování distribuované sítě pro publikování/odběr" na stránce 70 a "Klastrování publikování/odběru: Nejlepší postupy" na stránce 89.

Obecně platí, že obě topologie klastru poskytují následující výhody:

- Jednoduchá konfigurace v horní části topologie klastru po pevné lince.
- Automatická manipulace se správci front připojovaných a opouštějících klastr.
- Snadné rozšiřování pro další odběry a vydavatele tím, že přidávají další správce front a distribuují další odběry a vydavatele.

Tyto dvě topologie však mají různé výhody, protože požadavky jsou specifičtější.

Klastry s přímým směrováním publikování/odběru

Při přímém směrování odesílá každý správce front v klastru publikování z připojených aplikací přímo do libovolného jiného správce front v klastru s odpovídajícím odběrem.

Klastr publikování/odběru se směrováním poskytuje následující výhody:

- Zprávy určené pro odběr u konkrétního správce front ve stejném klastru jsou transportovány přímo do tohoto správce front a není nutné předávat intermediačního správce front. To může zlepšit výkon v porovnání s topologií hostitele určitého tématu nebo s topologickou topologií.
- Protože všichni správci front jsou k sobě navzájem přímo připojeni, neexistuje v rámci infrastruktury směrování této topologie jediný bod selhání. Není-li k dispozici jeden správce front, budou odběry ostatních správců front v klastru i nadále moci přijímat zprávy od vydavatelů k dostupným správcům front.
- Je velmi jednoduché nakonfigurovat, zejména na existujícím klastru.

Věci, které je třeba vzít v úvahu při použití klastru publikování/odběru s přímým směrováním:

- Všichni správci front v klastru se dozví o všech ostatních správcích front v klastru.
- Správci front v klastru, který je hostitelem jednoho nebo více odběrů v klastrovaném tématu, automaticky vytvářejí odesílací kanály klastru pro všechny ostatní správce front v klastru, a to ani v případě, že tito správci front nepublikují zprávy pro některá klastrovaná témata.
- První odběr ze správce front do řetězce tématu pod klastrovaným tématem vede k odeslání zprávy všem ostatním správcům front v klastru. Podobně i poslední odběr na řetězci tématu, který má být odstraněn, má za následek také zprávu. Čím více jednotlivých řetězců témat je používáno v rámci klastrovaného tématu, a čím vyšší je rychlost změn odběrů, tím více probíhá komunikace mezi správci front.
- Každý správce front v klastru uchovává znalosti odebíraných řetězců témat, o kterých je informován, a to i v případě, že správce front není ani publikující, ani přihlášení k odběru těchto témat.

Z výše uvedených důvodů budou všichni správci front v klastru s definovaným přímým směrovaným tématem vynakládat další režii. Čím více správců front je v klastru, tím větší je režie. Čím více témat témat se přihlásí a čím větší je jejich míra změny, tím větší je režie. To může vést k příliš velkému zatížení správců front spuštěných na malých systémech ve velkém nebo dynamickém klastru publikování/odběru s přímým směrováním. Další informace najdete v tématu Přímý směrovaný výkon publikování/odběru .

Když víte, že klastr nemůže pojmout režii přímého routed publish/subscribe, můžete místo toho použít hosted routed publish/subscribe. Alternativně můžete v extrémních situacích zcela vypnout funkce klastrovaných publikování/odběru nastavením atributu správce front **PSCLUS** na hodnotu DISABLED na každém správci front v daném klastru. Viz “Blokující publish/odběr v klastru” na stránce 99. Tím zabráníte vytvoření jakéhokoli klastrového tématu, a proto je zajištěno, že vaše síť nezpůsobuje žádné režijní náklady spojené s klastrovanými publikaci/přihlášením k odběru.

Klastry publikování/odběru hostitele tématu Topic

Při směrování hostitelů témat jsou správci front, ve kterých jsou klastrovaná témata, administrativně definovány, aby se staly směrovači pro publikace. Publikace z nehostujících správců front v klastru jsou směrovány přes hostitele správce front do libovolného správce front v klastru s odpovídajícím odběrem.

Klastr publikování/odběru se směrovaným hostitelem tématu poskytuje následující výhody nad přímým směrovaným klastrem publikování/odběru:

- Pouze správci front, na kterých jsou definována témata směrování na téma hostitele, jsou seznámeli se všemi ostatními správci front v klastru.
- Pouze správci front hostitele tématu musí být schopni připojit se ke všem ostatním správcům front v klastru a budou se obvykle připojovat pouze k těm, kde existují odběry. Mezi správci front proto dochází k výraznému snížení počtu kanálů.
- Správci front klastru, kteří jsou hostiteli jednoho nebo více odběrů v klastrovaném tématu, automaticky vytvářejí odesílací kanály klastru pouze u správců front, kteří jsou hostiteli tématu klastru, který je mapován na řetězec tématu odběru.
- První odběr ze správce front do řetězce tématu v rámci klastrovaného tématu má za následek odeslání zprávy správci front v klastru, který je hostitelem klastrovaného tématu. Podobně i poslední odběr na řetězci tématu, který má být odstraněn, má za následek také zprávu. Čím více jednotlivých řetězců témat je používáno v rámci klastrovaného tématu, a čím vyšší je četnost změn odběrů, tím více komunikace mezi správci front probíhá, ale pouze mezi hostiteli odběru a hostiteli témat.

- Větší kontrola nad fyzickou konfigurací. Se přímým směrováním se musí všichni správci front podílet na klastru publikování/odběru, čímž se zvyšují jejich režijní náklady. Při použití směrování hostitele témat jsou k dispozici pouze správci front hostitele témat o jiných správcích front a jejich odběry. Výslovně vyberete správce front hostitele tématu, proto můžete zajistit, aby tito správci front byli spuštění na odpovídajícím vybavení, a že pro ostatní správce front můžete používat méně výkonné systémy.

Co je třeba zvážit při použití klastru publikování/odběru se směrováním hostitele tématu:

- Další "přechod" mezi správcem front publikování a přihlášeným správcem front je představen, když není vydavatel nebo odběratel umístěn v tématu, který je hostitelem správce front. Latence způsobená dodatečným "přechodem" může znamenat, že směrování hostitele témat je méně účinné než přímé směrování.
- U velkých klastrů, směrování hostitele témat usnadňuje významné výkonnosti a škálování problémů, které můžete získat s přímým směrováním.
- Můžete se rozhodnout definovat všechna svá témata v jediném správci front nebo na velmi malém počtu správců front. Provedete-li to, ujistěte se, že jsou správci front hostitele témat hostováni na výkonných systémech s dobrou konektivitou.
- Stejné téma můžete definovat ve více než jednom správci front. Tím se zlepšuje dostupnost tématu a také zlepšuje rozšiřitelnost, protože IBM MQ pracovní zátěž vyvažuje publikace pro určité téma ve všech hostitelích pro dané téma. Všimněte si však, že definování stejného tématu ve více než jednom správci front ztratí pořadí zpráv pro dané téma.
- Díky hostování různých témat v různých správcích front můžete zlepšit rozšiřitelnost bez ztráty pořadí zpráv.

Související úlohy

Konfigurace klastru publikování/odběru

Ladění distribuovaných sítí typu publikování/odběr

Odstraňování problémů distribuovaného publikování/odběru

Související odkazy

Scénář pro klastr publikování/odběru

Přímé směrování v klastrech publikování/odběru

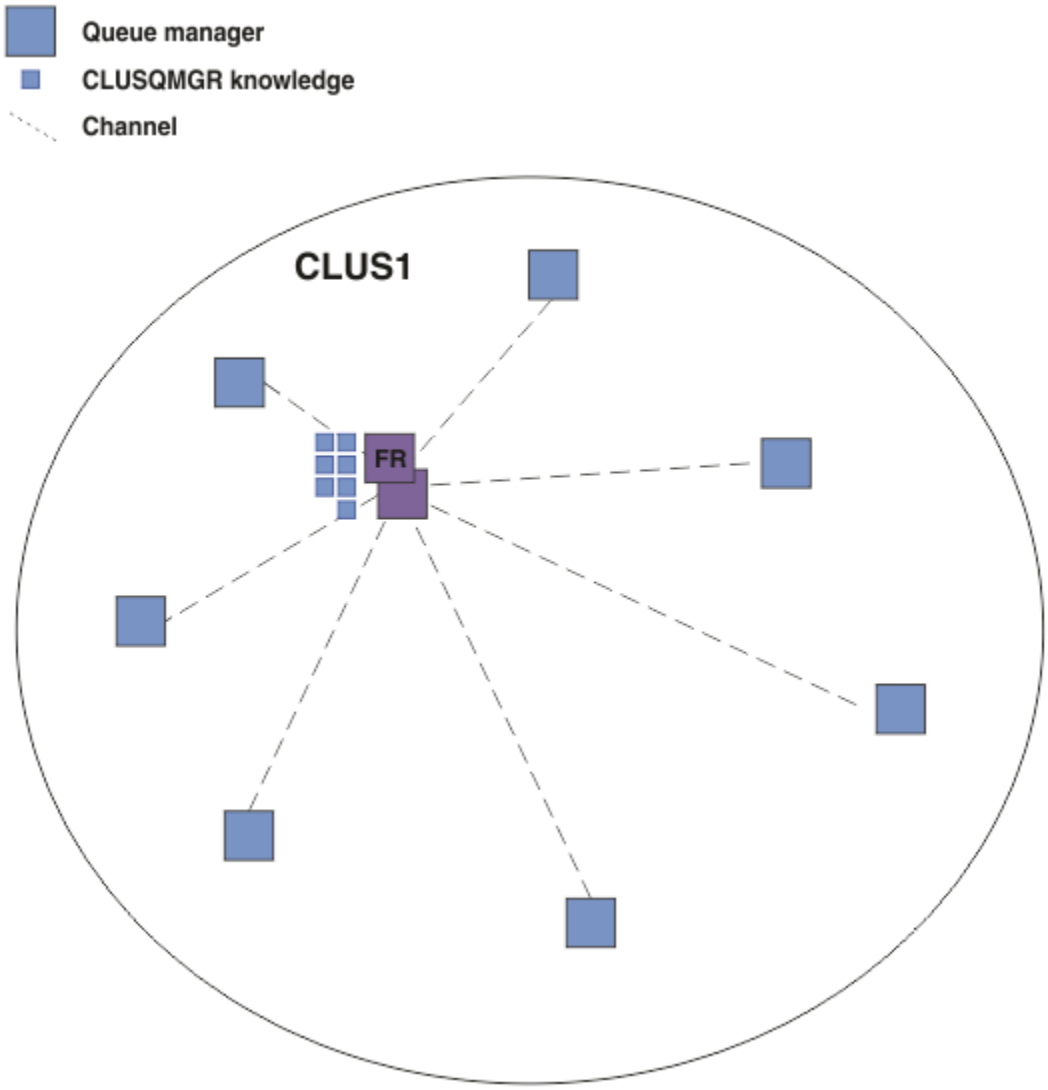
Publikace z libovolného správce front publikování jsou směrovány přímo na jiného správce front v klastru s odpovídajícím odběrem.

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.

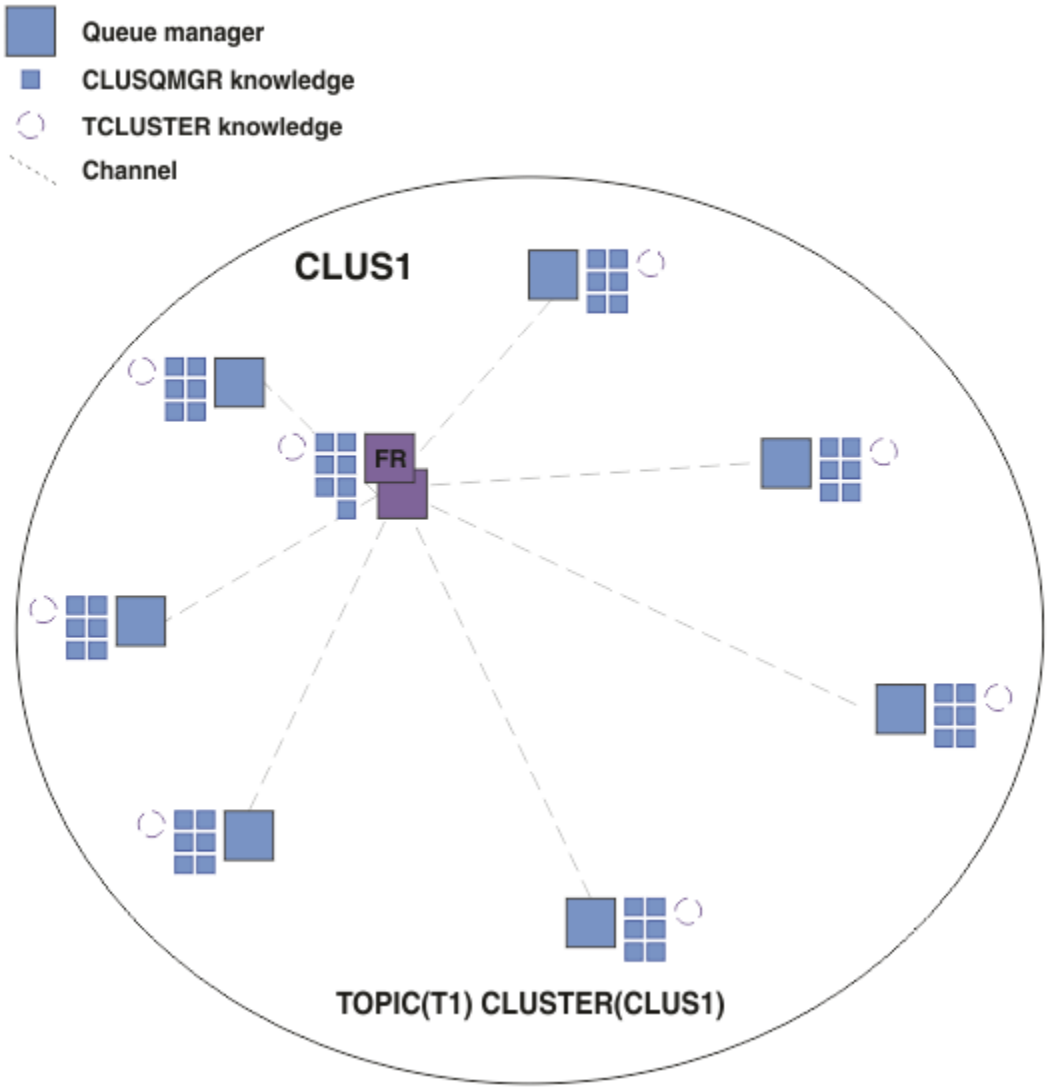
Následující diagram zobrazuje klastr správců front, který se aktuálně nepoužívá pro aktivity publikování/odběru nebo dvoubodové aktivity. Uvědomte si, že každý správce front v klastru se připojuje pouze ke správcům front úplného úložiště a z nich.



Obrázek 16. Klastr správců front

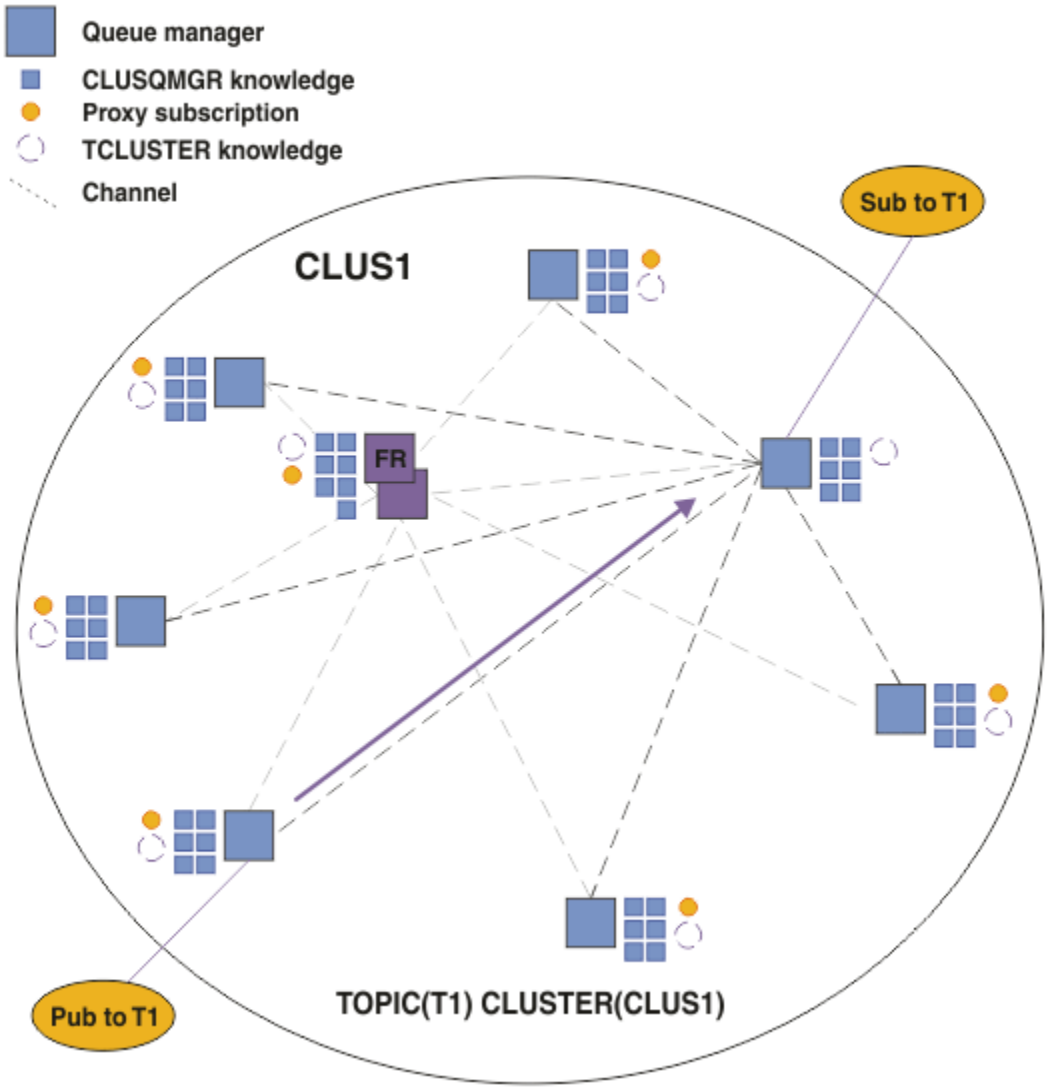
V případě publikování, která mají proudit mezi správci front v klastru s přímým směrováním, můžete vytvořit klastr pro větev stromu témat, jak je popsáno v tématu Konfigurace klastru publikování/odběru, a určit *přímé směrování* (výchozí nastavení).

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

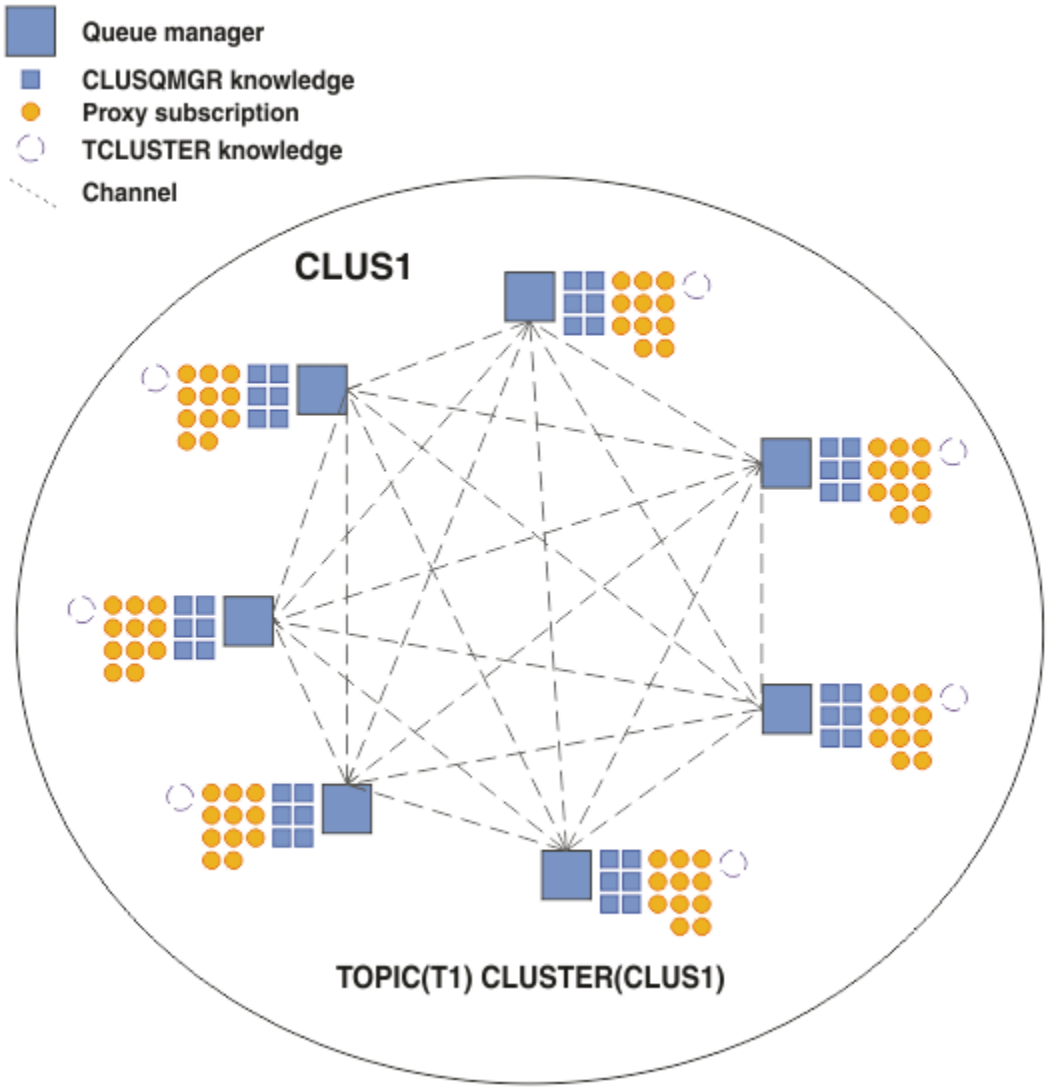
Při vytvoření odběru vytvoří správce front, který je hostitelem odběru, kanál pro každého správce front v klastru a odešle podrobnosti o odběru. Tyto znalosti distribuovaného odběru jsou reprezentovány proxy odběrem v jednotlivých správcích front. Při vytváření publikování v libovolném správci front 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 propojené povaze správců front publikování/odběru je třeba, aby se proxy odběry rozšířily na všechny uzly v síti. Vzdálené publikace nemusí být nutně odebírané okamžitě, takže časné publikace nemusí být odeslány na základě odběru nového řetězce tématu. Problémy způsobené prodlevou odběru můžete odstranit tím, že budou všechny publikace šířeny pro všechny správce front, což odstraňuje nutnost proxy odběrů. Viz téma Výkon odběru v sítích typu publikování/odběr.

  Poznámka: Toto omezení platí také pro hierarchie.

Před použitím přímého směrování prozkoumejte alternativní přístupy popsané v části "Směrování hostitele témat v klastrech publikování/odběru" na stránce 80a "Směrování v hierarchiích publikování/odběru" na stránce 103.

Směrování hostitele témat v klastrech publikování/odběru

Publikace z nehostujících správců front v klastru jsou směrovány přes hostitele správce front do libovolného správce front v klastru s odpovídajícím odběrem.

Úvod do způsobu, jakým jsou zprávy směrovány mezi správci front v hierarchiích publikování a odběru a v klastrech, najdete v tématu Distribuované sítě typu publikování/odběr.

Chcete-li porozumět chování a přínosům směrování hostitele témat, je nejlepší nejprve porozumět produktu "Přímé směrování v klastrech publikování/odběru" na stránce 75.

Klastr publikování/odběru se směrovaným hostitelem tématu se chová takto:

- Klastrované spravované objekty témat jsou ručně definovány v jednotlivých správcích front v klastru. Na tyto informace se odkazuje jako na *správce front hostitele tématu*.
- Je-li proveden odběr ve správci front klastru, jsou kanály vytvořeny ze správce front hostitele odběru na správce front hostitele tématu a proxy odběry jsou vytvářeny pouze ve správcích front, které jsou hostiteli daného tématu.
- Když aplikace publikuje informace do tématu, vždy připojený správce front postoupí publikování jednomu správci front, který je hostitelem tématu, a předá jej všem správcům front v klastru, kteří mají odpovídající odběry daného tématu.

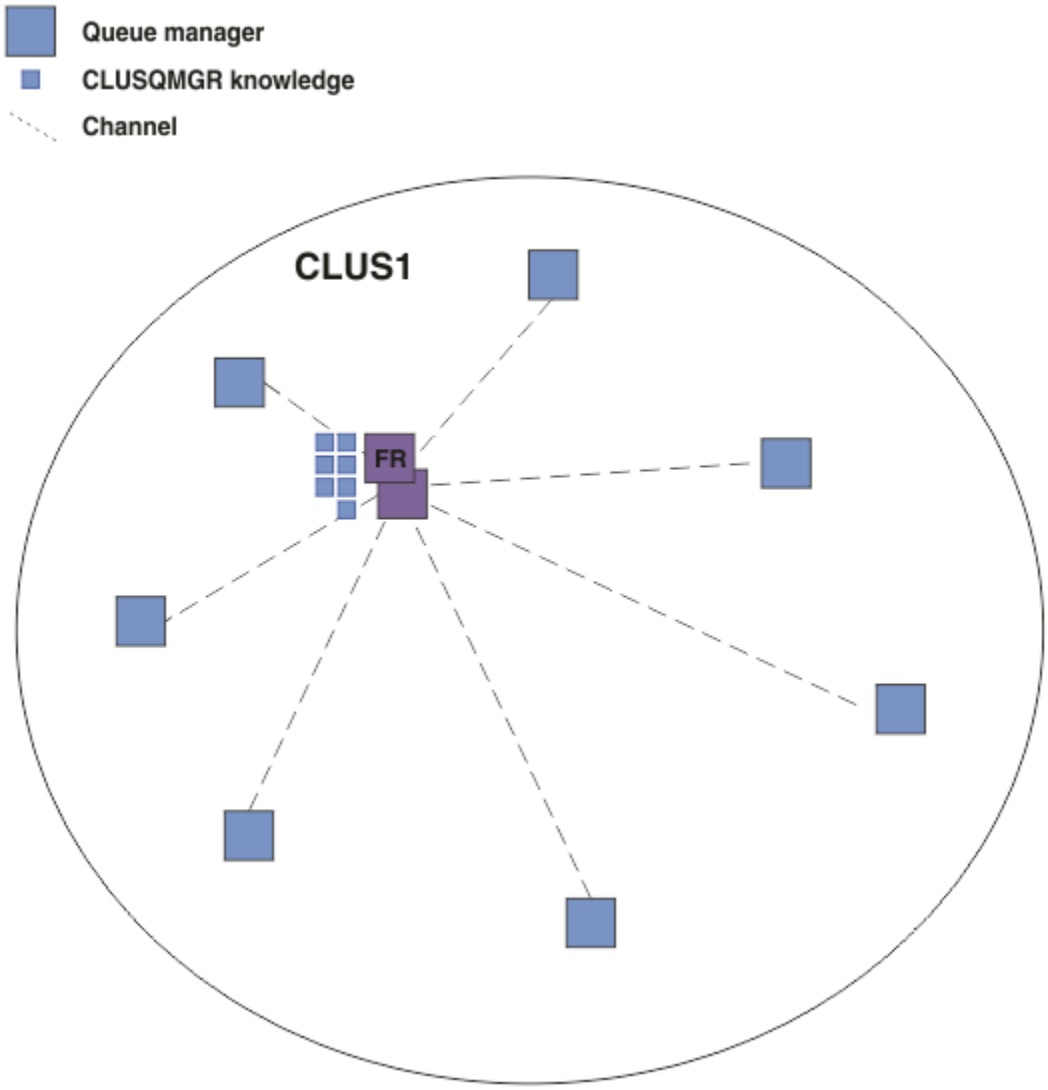
Tento proces je podrobněji vysvětlen v následujících příkladech.

Směrování hostitele tématu pomocí jednoho hostitele témat

V případě publikací k toku mezi správci front v klastru se směrovaným hostitelem témat můžete klastrovou větev stromu témat, jak je popsáno v tématu Konfigurace klastru publikování/odběru, a zadejte téma *Směrování hostitele témat*.

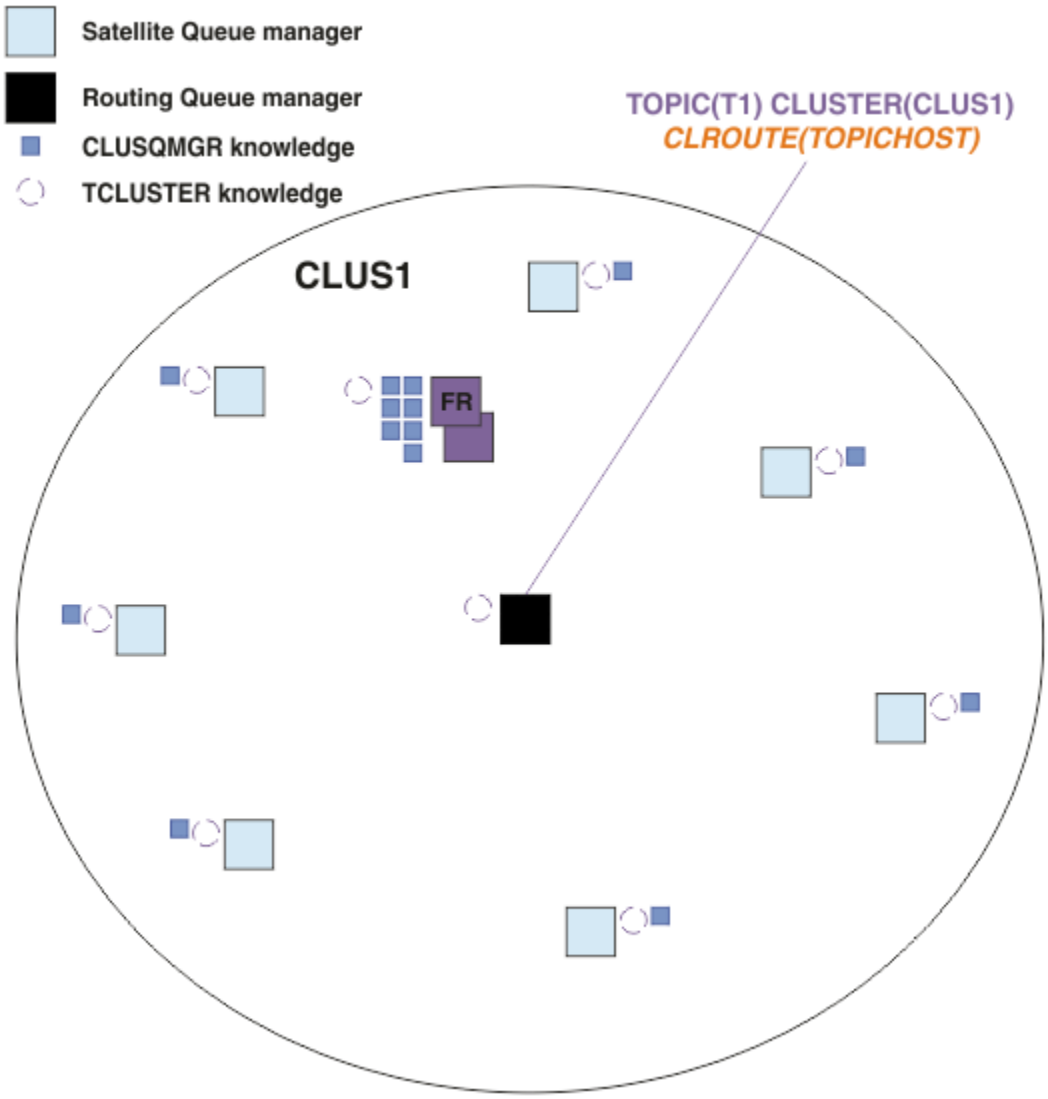
Existuje mnoho důvodů k definování objektu tématu směrování hostitele témat ve více správcích front v klastru. Nicméně pro zjednodušení začneme s jedním hostitelem tématu.

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.



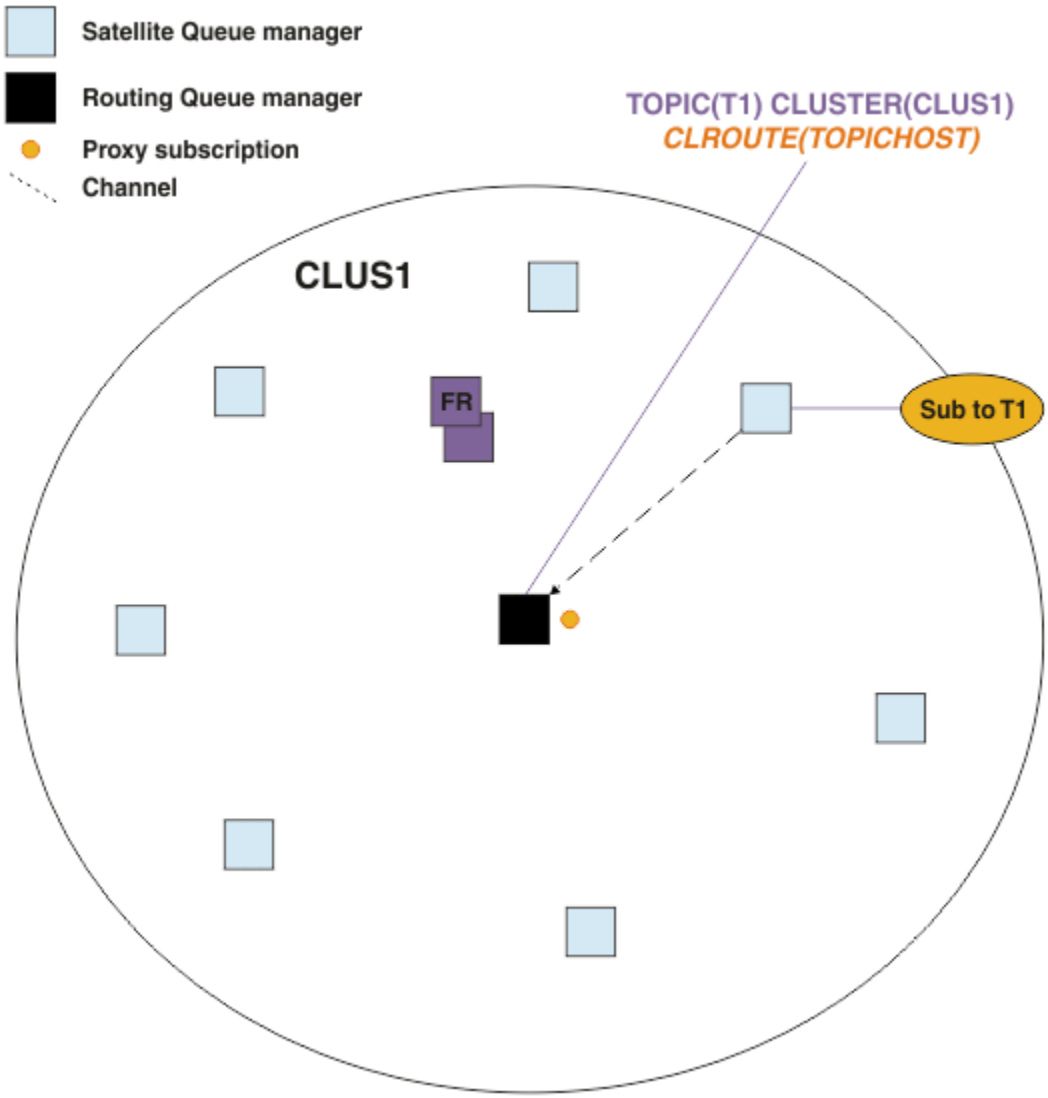
Obrázek 20. Klastr správců front

V klastru publikování/odběru se směrovaným hostitelem témat definujte objekt tématu ve specifickém správci front v daném klastru. Přenos publikování/odběru poté prochází daným správcem front, takže je v klastru kritickým správcem front a zvyšuje jeho pracovní zátěž. Z těchto důvodů se nedoporučuje používat správce front úplného úložiště, ale k použití jiného správce front v klastru. Definujete-li objekt tématu ve správci front hostitele, budou všichni ostatní správci front v klastru automaticky prosazovány znalostmi daného objektu a jeho hostitele všemi ostatními správci front v úložišti. Všimněte si, že na rozdíl od *přímého směrování*není každý správce front o každém dalším správci front v klastru informován.



Obrázek 21. Klastr publikování/odběru se směrovaným klastrem publikování/odběru s jedním tématem definovaným na jednom hostiteli tématu

Je-li vytvořen odběr ve správci front, vytvoří se kanál mezi správcem front odběru a správcem front hostitele tématu. Správce front odběru 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 žádných dalších správců front v klastru.

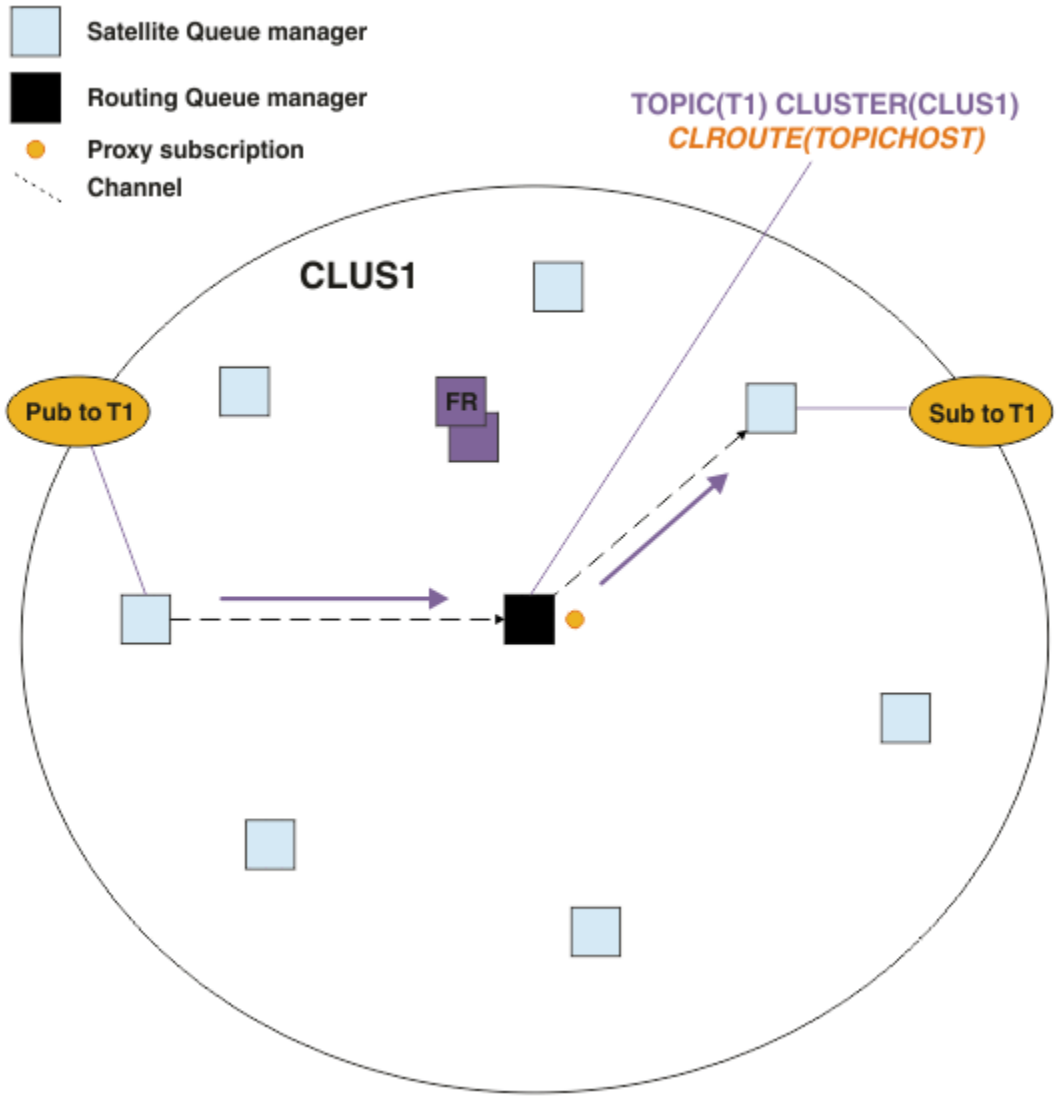


Obrázek 22. Klastr publikování/odběru se směrovaným klastrem publikování/odběru s jedním tématem definovaným na jednom hostiteli témat a jedním odběratelem

Když se publikační aplikace připojí k jinému správci front a je publikována zpráva, dojde k vytvoření kanálu mezi správcem front publikování a správcem front hostitele tématu a zpráva se předá tomuto správci front. Publikační správce front nemá žádné znalosti o odběrech jiných správců front v klastru, takže je zpráva předávána správci front hostitele tématu i v případě, že v klastru nejsou žádní odběratelé tohoto tématu. Správce front publikování se připojí pouze ke správci front hostitele tématu. Publikace jsou směrovány přes hostitele témat do odebírajících správců front, pokud existují.

Odběry ve stejném správci front, jako je vydavatel, jsou spokojeni přímo, aniž by nejprve odesílali zprávy do správce front hostitele tématu.

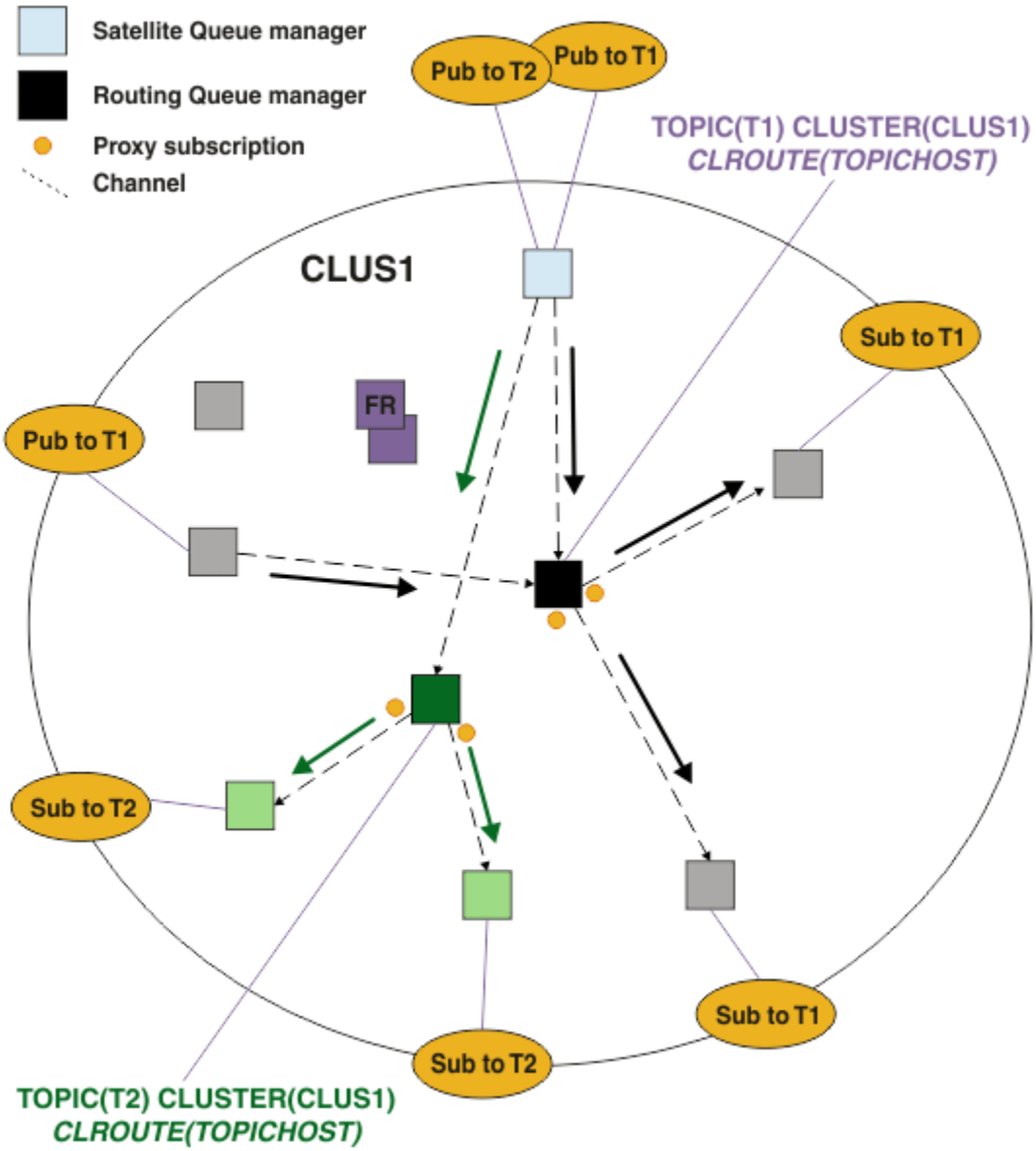
Všimněte si, že vzhledem ke kritické roli, kterou hraje každý správce front hostitele tématu, musíte zvolit správce front, kteří mohou pracovat s požadavky na načtení, dostupnost a konektivitu tématu hosting.



Obrázek 23. Klastr publikování/odběru se směrovaným publikováním tématu s jedním tématem, jedním odběratelem a jedním vydavatelem.

Rozdělení stromu témat na více správců front

Srouted topic hosting queue manager is only responsible for the subscription knowledge and publication messages that relate to the branch of the topic tree that its administered topic object is configured for. Jsou-li v různých aplikacích pro publikování/odběr v klastru použita různá témata, můžete nakonfigurovat různé správce front tak, aby hostují různé klastrové větve stromu témat. To umožňuje škálování snížením provozu publikování, znalostí odběru a kanálů na každém správci front hostitele témat v klastru. Tuto metodu byste měli používat pro různé větve s vysokým objemem daného stromu témat:



Obrázek 24. Klastr publikování/odběru se dvěma tématy, každý z nich definovaný na jednom hostiteli témat.

Například při použití témat popisovaných v tématu Stromy témat, pokud bylo téma T1 konfigurováno s řetězcem tématu `/USA/Alabamaa` téma T2 bylo konfigurováno s řetězcem tématu `/USA/Alaska`, byla by zpráva publikovaná do produktu `/USA/Alabama/Mobile` směrována prostřednictvím správce front hostujícího T1, a zpráva publikovaná do produktu `/USA/Alaska/Juneau` by byla směrována přes správce front hostujícího T2.

Poznámka: Nelze vytvořit jediné předplatné více klastrovaných větví stromu témat pomocí zástupného znaku vyššího ve stromu témat, než jsou body, které jsou klastrované. Viz téma Odběry zástupných znaků.

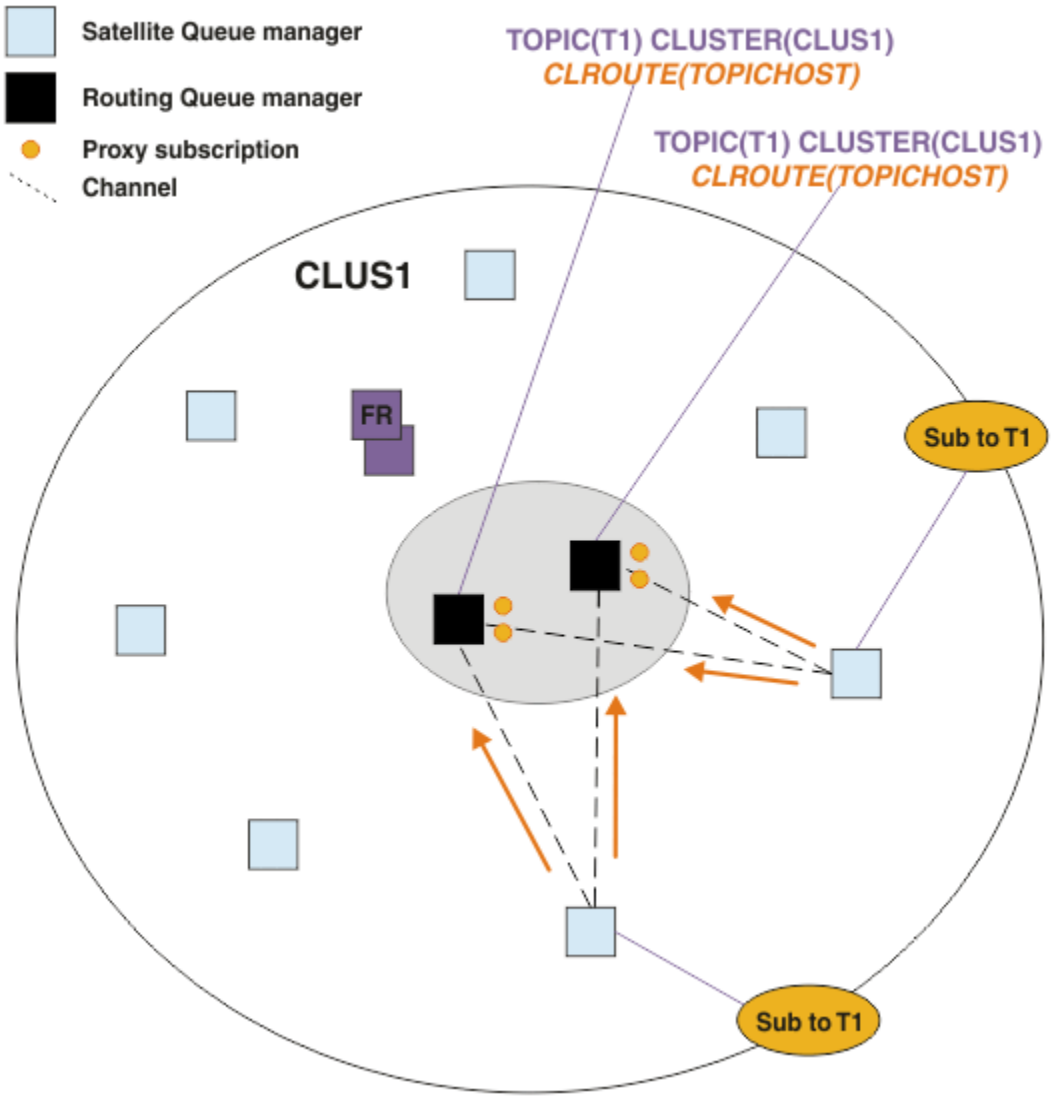
Směrování hostitele témat pomocí více hostitelů témat pro jedno téma

Má-li jeden správce front zodpovědnost za směrování tématu a tento správce front přestane být k dispozici nebo není schopen zpracovávat pracovní zátěž, nebudou publikování rychle odtéci do odběrů.

Potřebujete-li větší odolnost, rozšiřitelnost a vyrovnávání pracovní zátěže, než jste získali při definování tématu v jednom jediném správci front, můžete definovat téma ve více než jednom správci front. Každá jednotlivá publikovaná zpráva je směrována prostřednictvím jednoho hostitele témat. Existuje-li více odpovídajících definic hostitele témat, je vybrán jeden z hostitelů témat. Tato volba je provedena stejným

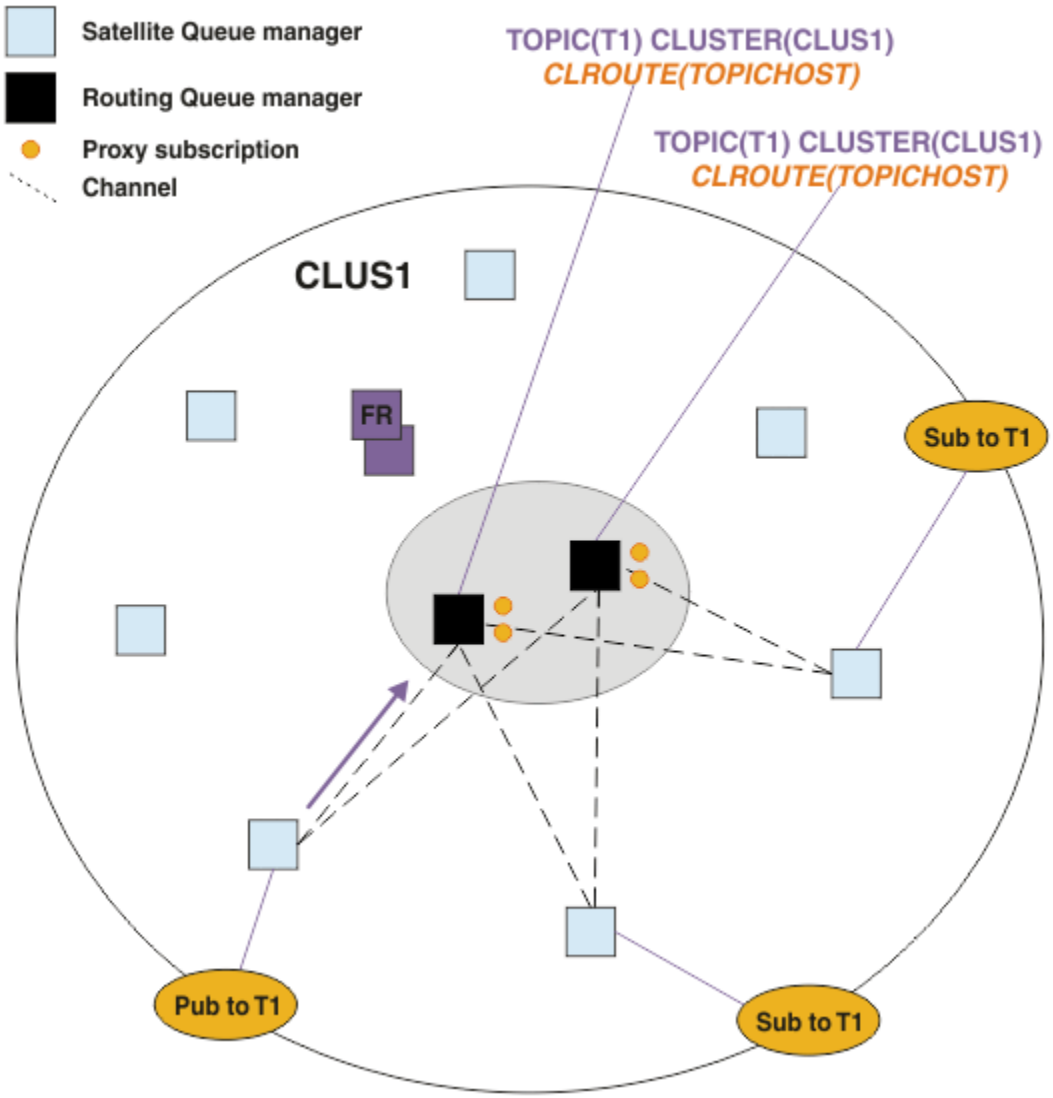
způsobem jako u klastrovaných front. To umožňuje směrovat zprávy k dostupným hostitelům témat, vyhnout se všem, které nejsou k dispozici, a umožňuje vyrovnávání pracovní zátěže zátěže ve více správcích front hostitele a kanálů hostitele. Avšak řazení přes více zpráv se nezachová, když použijete více hostitelů témat pro stejné téma v klastru.

Následující diagram zobrazuje klastr se směrovaným hostitelem témat, ve kterém bylo definováno stejné téma ve dvou správcích front. V tomto příkladu odesílají správci front odběru informace o odebíraných tématech do správců front hostitele tématu v podobě odběru proxy:



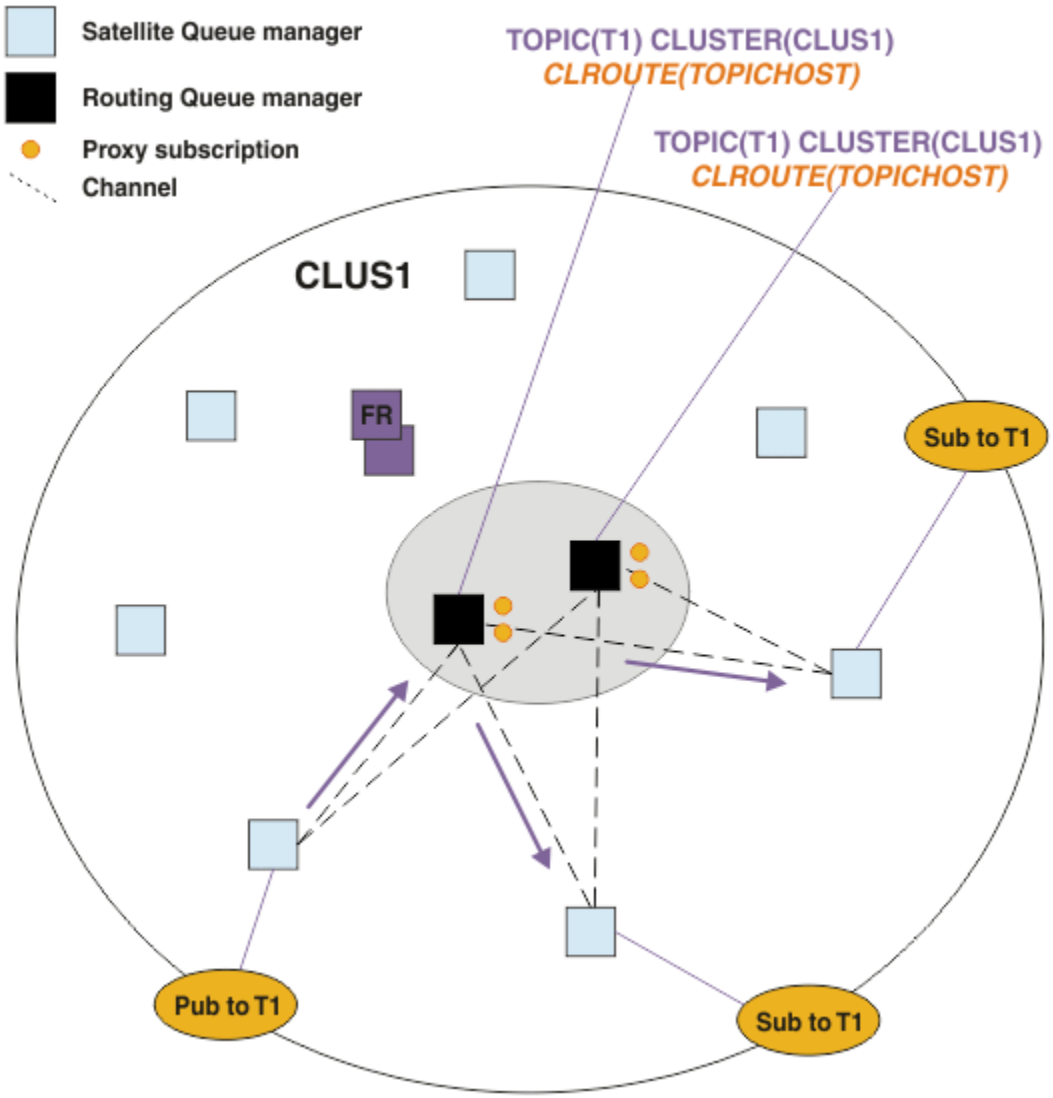
Obrázek 25. Vytvoření proxy odběrů v klastru publikování/odběru hostitele s více tématy

Je-li publikace vytvořena z nehostujícího správce front, odešle správce front kopii publikace do *jednoho* z správců front hostitele tématu pro dané téma. Systém zvolí hostitele na základě výchozího chování algoritmu správy pracovní zátěže klastru. V typickém systému se tato hodnota blíží rozdělení typu round-robin v rámci každého správce front hostitele tématu. Neexistuje žádná afinita mezi zprávami ze stejné aplikace publikování. Tato hodnota se rovná použití typu vazby klastru `NOTFIXED`.



Obrázek 26. Příjem publikování v klastru publikování/odběru hostitele s více tématy

Příchozí publikace ve vybraném správci front hostitele tématu jsou poté předány všem správcům front, kteří zaregistrovali odpovídající odběr serveru proxy:



Obrázek 27. Směrování publikování pro odběratele v klastru publikování/odběru hostitele více témat

Vytváření odběrů a vydavatelů lokálních pro správce front hostitele tématu

Výše uvedené příklady ukazují směrování mezi vydavateli a odběrateli ve správcích front, kteří nejsou hosteli administrovaných objektů tématu. V těchto topologiích vyžadují zprávy více *přechodů* k dosažení odběrů.

Není-li další přechod žádoucí, může být vhodné připojit vydavatele klíčů k tématu hostujícím správce front. Pokud však existuje více hostitelů témat pro určité téma a pouze jeden vydavatel, bude veškerý publikační provoz směrován přes správce front hostitele tématu, ke kterému je vydavatel připojen.

Podobně platí, že pokud existují odběry klíčů, mohou být umístěny ve správci front hostitele tématu. Pokud však existuje více hostitelů směrovaných témat, pouze část publikací se vyhnete dalšímu směrovacímu uzlu, přičemž zbytek bude nejprve směrován přes ostatní správce front hostitele tématu.

Topologie, jako jsou tyto, jsou popsány dále: Směrování hostitele tématu pomocí centralizovaných vydavatelů nebo odběratelů.

Poznámka: Při změně směrované konfigurace tématu při společném vyhledávání vydavatelů nebo odběrů se směrovanými hostitelskými tématy je třeba speciální plánování. Příklad naleznete v tématu Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu.

Souhrn a další pokyny

Klastr publikování/odběru se směrovaným hostitelem tématu vám poskytuje přesnou kontrolu nad tím, které správce front hostí každé téma, a tito správci front se stávají správci front *směrování* pro danou větev stromu témat. Kromě toho správci front bez odběrů a vydavatelů nepotřebují navázat spojení s hostitelskými správci front tématu a správci front s odběry nemusí být připojeni 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, ve kterých se provádí publikování/odběr pouze v podmnožině správců front. Tato konfigurace vám také poskytuje kontrolu nad zátěží na jednotlivých správcích front v klastru, takže (například) můžete zvolit, že chcete hostit vysoce aktivní témata na výkonnějších a odolnějších systémech. Pro určité konfigurace-zejména 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 výše, může toto riziko zmírnit vydavatelé lokální vzhledem k hostiteli tématu.
- 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 již bylo popsáno výše, může toto riziko zmírnit odběry nebo vydavatelé lokální pro určitého hostitele témat.
- 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.

Dříve než použijete směrování hostitele témat, prozkoumejte alternativní přístupy podrobně popsané v části “Přímé směrování v klastrech publikování/odběru” na stránce 75a “Směrování v hierarchiích publikování/odběru” na stránce 103.

Klastrování publikování/odběru: Nejlepší postupy

Použití klastrovaných témat rozšiřuje doménu publikování/odběru mezi správci front jednoduchou, ale může vést k problémům, pokud se mechanici a implikace plně nerozumí. Pro sdílení informací a směrování publikací existují dva modely. Implementujte model, který nejlépe vyhovuje vašim individuálním obchodním potřebám, a nejlepší na vybraném klastru.

Informace o nejlepších postupech v následujících sekcích nepřinášejí žádné řešení pro všechny řešení, ale spíše sdílí společné přístupy k řešení běžných problémů. Předpokládá se, že máte základní informace o klastrech IBM MQ a systému zpráv publikování/odběru, a že jste obeznámeni s informacemi v části Distribuované sítě publikování/odběru a “Návrh klastrů publikování a odběru” na stránce 73.

Pokud používáte klastr pro systém zpráv typu point-to-point, každý správce front v klastru pracuje na potřebách-to-know-to-know-to-know. To znamená, že se nachází pouze o dalších klastrových prostředcích, jako jsou například ostatní správci front v klastru a klastrované fronty, když se k nim aplikace

připojují. Přidáte-li do klastru systém zpráv typu publikování/odběr, bude představen vyšší úroveň sdílení informací a konektivity mezi správci front klastru. Chcete-li být schopni dodržovat doporučené postupy pro klastry publikování/odběru, musíte plně pochopit důsledky této změny chování.

Chcete-li umožnit sestavení nejlepší architektury založené na vašich přesných potřebách, existují dva modely pro sdílení informací a směrování publikování v klastrech publikování/odběru: *přímé směrování* a *směrování hostitele témat*. Chcete-li učinit správnou volbu, musíte pochopit oba modely, a různé požadavky, které každý model splňuje. Tyto požadavky jsou popsány v následujících sekcích ve spojení s produktem "Plánování distribuované sítě pro publikování/odběr" na stránce 70:

- "Důvody k omezení počtu správců front klastru zahrnutých do aktivity publikování/odběru" na stránce 90
- "Jak rozhodnout, která témata do klastru" na stránce 90
- "Jak nastavit velikost systému" na stránce 91
- "Umístění vydavatele a odběru" na stránce 92
- "Provoz publikování" na stránce 92
- "Změna odběru a dynamické řetězce témat" na stránce 93

Důvody k omezení počtu správců front klastru zahrnutých do aktivity publikování/odběru

Při použití systému zpráv publikování/odběru v klastru se používají pokyny týkající se kapacity a výkonu. Proto je vhodné pečlivě zvážit potřebu aktivity publikování/odběru u správců front a omezit ji pouze na počet správců front, kteří ji vyžadují. Po určení minimální sady správců front, kteří potřebují publikovat a odebírat témata, je možné vytvořit členy klastru, který obsahuje pouze tyto informace, a ne ostatní správce front.

Tento přístup je zvláště užitečný, máte-li již fungující klastr dobře fungující pro systém zpráv typu point-to-point. Při převrácení existujícího velkého klastru do klastru publikování/odběru je lepší nejprve vytvořit samostatný klastr pro práci publikování/odběru, kde se mohou aplikace pokusit o práci, místo použití aktuálního klastru. Můžete použít podmnožinu existujících správců front, kteří jsou již v jednom nebo více klastrech mezi dvěma body, a vytvořit z těchto dílčích sad členy nového klastru publikování/odběru. Správci front úplného úložiště pro váš nový klastr však nesmí být členy žádného jiného klastru. Toto izoluje přídavnou zátěž od existujících úplných úložišť klastru.

Pokud nemůžete vytvořit nový klastr a chcete-li převést existující velký klastr na klastr publikování/odběru, nepoužívejte přímý směrovaný model. Model routed Host routed se obvykle provádí lépe ve větších klastrech, protože obecně omezuje sdílení informací publikování/odběru a propojitelnost se sadou správců front, kteří aktivně provádějí práci publikování/odběru a soustřeďují se na správce front, který je hostitelem témat. Výjimkou je, je-li vyvolána ruční aktualizace informací o odběrech ve správci front, který je hostitelem definice tématu, v tomto momentu se správce front hostitele tématu připojí ke každému správci front v klastru. Viz téma Opětovná synchronizace proxy odběrů.

Určíte-li, že klastr nelze použít pro publikování/odběr v důsledku jeho velikosti nebo aktuálního načtení, je dobrým zvykem zabránit tomu, aby se tento klastr neočekávaně dostal do klastru publikování/odběru. Pomocí vlastnosti správce front produktu **PSCLUS** můžete zabránit komukoli přidáním klastrovaného tématu do libovolného správce front v klastru. Viz "Blokující publish/odběr v klastru" na stránce 99.

Jak rozhodnout, která témata do klastru

Je důležité si pečlivě vybrat, která témata se přidají do klastru: Čím vyšší je tato témata, tím více se jejich použití stává. To může vést k většímu šíření informací o odběru a publikování, než je nezbytné. Existuje-li více různých větví stromu témat, kde některé je třeba dělit do klastrů a některé nikoli, vytvořte spravované objekty témat v kořenovém adresáři každé větve, která potřebuje klastrování, a přidejte je do klastru. Například, pokud větve `/A`, `/B` a `/C` vyžadují klastrování, definujte samostatné klastrované objekty témat pro každou větev.

Poznámka: Systém vám zabrání vnořování definic sdružených témat ve stromu témat. Jste oprávněni pouze ke klastrovaných tématech v jednom bodě stromu témat pro každou podvětev. Například nemůžete

definovat klastrované objekty témat pro /A a pro /A/B. Vnoření klastrovaných témat může vést k nejasnostem ohledně toho, který klastrovaný objekt platí pro daný odběr, zvláště v případech, kdy odběry používají zástupné znaky. To je ještě důležitější při použití směrování hostitele témat, kde jsou rozhodnutí směrování přesně definována vaším přidělením hostitelům tématu.

Pokud je třeba do stromu témat přidat klastrovaná témata, ale některé větve stromu pod klastrovaným bodem nevyžadují klastrované chování, můžete použít atributy rozsahu odběru a rozsahu publikování, abyste snížili úroveň sdílení odběru a publikování pro další témata.

Neměli byste umístit kořenový uzel tématu do klastru, aniž byste uvažovali o chování, které je vidět. Je-li to možné, musí být globální témata zřejmá, například pomocí kvalifikátoru vyšší úrovně v řetězci tématu: `/global` nebo `/cluster`.

Existuje další důvod, proč nechcete, aby byl uzel kořenového tématu rozdělen do klastrů. Důvodem je to, že každý správce front má lokální definici pro kořenový uzel, objekt tématu produktu `SYSTEM.BASE.TOPIC` . Je-li tento objekt klastrován v jednom správci front v klastru, jsou o něm informováni všichni ostatní správci front. Avšak když existuje lokální definice stejného objektu, její vlastnosti potlačují objekt klastru. Výsledkem je to, že tito správci front jednají tak, jako by se neklastrovaných témat neklastrovaných. Chcete-li tento problém vyřešit, je třeba použít klastr pro každou definici `SYSTEM.BASE.TOPIC`. Můžete to udělat pro přímé směrované definice, ale ne pro definice směrovaných hostitelů témat, protože způsobí, že se každý správce front stane hostem tématu.

Jak nastavit velikost systému

Klastry publikování/odběru obvykle vedou k odlišnému vzoru kanálů klastru pro výměnu zpráv mezi dvěma body v klastru. Model dvoubodového spojení je 'opt in', ale klastry pro publikování/odběr mají více nerozlišující charakter s rozpisem odběrů, zvláště při použití přímých směrovaných témat. Proto je důležité zjistit, kteří správci front v klastru publikování/odběru budou používat kanály klastru k připojení k jiným správcům front a za jakých okolností.

V následující tabulce jsou uvedeny typické sady odesílacích kanálů klastru a přijímacích kanálů očekávané pro jednotlivé správce front v klastru publikování/odběru v rámci běžného spuštění, v závislosti na roli správce front v klastru publikování/odběru.

Tabulka 5. Odesílací kanál klastru a kanály příjemce pro každou metodu směrování.

Role správce front	**Přímé zásobníky klastru**	**Přímé odesilatelé klastru**	**Přijímače klastru témat**	**odesilatelé klastru 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)	Žádný (1)	Žádný (2)	Žádný (2)

Klíč:

AllQmgrs
Kanál pro všechny správce front v klastru a z něj.

AllSubs
Kanál pro všechny správce front, v němž byl vytvořen odběr, a z něj.

AllPubs
Kanál pro všechny správce front, ve kterém byla připojena publikující aplikace, a z nich.

AllHosts
Kanál pro všechny správce front, v němž byla konfigurována definice klastrovaného objektu tématu.

Není
Pro jediný účel publikování/odběru zpráv nejsou k dispozici žádné kanály pro správce front v klastru nebo z jiných správců front.

Notes:

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

Předchozí tabulka ukazuje, že směrování hostitele témat typicky používá výrazně méně odesílacích kanálů klastru a přijímacích kanálů než přímé směrování. Je-li konektivita kanálu důvodem pro určité správce front v klastru z důvodů kapacity nebo schopnosti vytvářet určité kanály (například prostřednictvím bran firewall), je upřednostňovaným řešením směrování hostitele témat.

Umístění vydavatele a odběru

Klastrované publikování/odběr umožňuje publikovat zprávy publikované na jednoho správce front do odběrů v libovolném jiném správci front v klastru. Co se týče systému zpráv typu point-to-point, mohou být náklady na přenos zpráv mezi správci front škodlivé pro výkon. Proto byste měli zvážit vytváření odběrů témat na stejných správcích front, jako jsou zprávy, které jsou publikovány.

Při použití směrování hostitele témat v rámci klastru je důležité také zvážit umístění odběrů a vydavatelů s ohledem na téma, které jsou hostiteli správců front. Není-li vydavatel připojen ke správci front, který je hostitelem klastrovaného tématu, publikované zprávy jsou vždy odesílány do tématu hostujícího správce front. Podobně platí, že je-li odběr vytvořen ve správci front, který není hostitelem tématu pro klastrované téma, jsou zprávy publikované z jiných správců front v klastru vždy odeslány do tématu hostujícího správce front jako první. Přesněji řečeno, pokud je odběr umístěn ve správci front, který je hostitelem daného tématu, ale existuje jeden nebo více správců front, kteří jsou hostiteli stejného tématu, je určitá část publikací z jiných správců front směrována prostřednictvím těchto dalších témat, která jsou hostitelem správců front. Další informace o návrhu klastru publikování/odběru s cílem minimalizovat vzdálenost mezi vydavateli a odběry naleznete v tématu Směrování hostitele tématu pomocí centralizovaných vydavatelů nebo odběratelů .

Provoz publikování

Zprávy publikované aplikací připojenou k jednomu správci front v klastru jsou přeneseny do odběrů v jiných správcích front prostřednictvím odesílacích kanálů klastru.

Když používáte přímé směrování, publikované zprávy přijímají nejkratší cestu mezi správci front. To znamená, že jdou přímo ze správce front publikování do každého správce front s odběry. Zprávy se nepřenášejí na správce front, kteří nemají odběry pro dané téma. Viz téma Odběry proxy v síti typu publikování/odběr.

Je-li rychlost zpráv publikování mezi jedním správcem front a jinou v klastru vysoká, musí být infrastruktura kanálu klastru mezi těmito dvěma body schopna udržet rychlost. To může zahrnovat vyladění použitých kanálů a přenosové fronty.

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

- Je přijatelná další latence první odeslání každé publikace do hostitelského správce front tématu?
- Může každý správce front hostitele udržovat příchozí a odchozí publikační sazbu? Zvažte použití systému s vydavateli v mnoha různých správcích front. Pokud všechny tyto zprávy odesílají do velmi malé sady témat, která jsou hostitelem správců front, mohou se tito témata stát kritickým místem při zpracování těchto zpráv a jejich přesměrováním do správců front, kteří jsou přihlášeni k odběru.
- Očekává se, že významný podíl publikovaných zpráv nebude mít k dispozici odpovídající odběratele? Je-li tomu tak, a míra publikování takových zpráv je vysoká, může být nejlepší nastavit správce front

vydavatele jako hostitele tématu. V takové situaci se žádná publikovaná zpráva, v níž neexistují žádné odběry v klastru, nebude přenášet na žádné jiné správce front.

Tyto problémy mohou být také zmírněno zavedením více hostitelů témat, aby se rozšířilo jejich načtení přes tyto problémy:

- Existuje-li více různých témat, každá z nich má podíl na přenosu publikování, zvažte jejich hostování na různých správcích front.
- Pokud témata nemohou být oddělena od různých hostitelů témat, zvažte definování stejného objektu tématu ve více správcích front. Výsledkem je, že publikace jsou v rámci každého z nich vyváženy pro směrování. To je však vhodné pouze v případě, že není vyžadováno pořadí publikování zpráv.

Změna odběru a dynamické řetězce témat

Další úvaha je vliv na výkon systému pro šíření proxy odběrů. Obvykle správce front odešle zprávu o odběru serveru proxy některým dalším správcům front v klastru, pokud je v daném správci front vytvořen první odběr specifického klastrovaného řetězce tématu (nikoli pouze konfigurovaný objekt tématu). Podobně se odešle zpráva o odstranění odběru proxy, když je odstraněn poslední odběr specifického klastrovaného tématu tématu.

Pro přímé směrování odesílá každý správce front s odběry tyto proxy odběry všem ostatním správcům front v klastru. Pro směrování hostitele témat každý správce front s odběry odešle pouze proxy odběry každému správci front, který je hostitelem definice pro dané klastrované téma. Díky přímému směrování jsou tím správci front v klastru vyšší, a tím vyšší je režie udržování proxy odběrů v rámci nich. Zatímco u směrování hostitele témat není počet správců front v klastru faktorem.

V obou modelech směrování se v případě, že se řešení publikování/odběru skládá z mnoha jedinečných řetězců témat, které jsou přihlášeny k odběru, nebo témata ve správci front v klastru jsou často odebíraná a odebíraná, bude na tomto správci front zaznamenána výrazná režie, způsobená stále generováním zpráv distribuujících a odstraňováním proxy odběrů. Je-li přímé směrování, je tato skutečnost spojena s nutností posílat tyto zprávy každému správci front v klastru.

Je-li četnost změn odběrů příliš vysoká, aby pojmula, dokonce i v rámci systému routed host, viz téma Výkon odběru v sítích publikování/odběru , kde najdete informace o způsobech snížení režie odběru proxy.

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.

Použijete-li přímé směrování, nebude umístění definice klastrovaného tématu přímo ovlivňovat chování systému, protože všichni správci front v klastru používají definici tématu stejným způsobem. Měli byste proto definovat téma ve všech správcích front, které budou členy klastru, dokud je dané téma potřeba, a že je na systému dostatečně spolehlivém, aby byl pravidelně ve styku se správci front úplného úložiště.

Používáte-li směrování hostitele témat, je umístění definice klastrovaného tématu velmi důležité, protože ostatní správci front v klastru vytvářejí kanály tohoto správce front a odesílají informace o odběru a publikacím. Chcete-li vybrat nejlepšího správce front, který má být hostitelem definice tématu, je třeba porozumět směrování hostitelů témat. Viz “Směrování hostitele témat v klastrech publikování/odběru” na stránce 80.

Máte-li klastrované téma a lokální objekt tématu, bude mít přednost lokální téma. Viz “Více definic témat klastru se stejným názvem” na stránce 96.

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

Dědění klastrovaného tématu

Publikování a přihlášení k odběru v klastrované topologii publikování/odběru obvykle předpokládá, že budou fungovat stejně, bez ohledu na správce front v klastru, k němuž jsou připojeny. To je důvod, proč jsou klastrované spravované objekty témat šířeny do každého správce front v klastru.

Spravovaný objekt tématu dědí chování od jiných spravovaných objektů témat ve stromu témat. Tato dědičnost nastane, když pro parametr tématu nebyla nastavena explicitní hodnota.

V případě klastrového publikování/odběru je důležité vzít v úvahu tuto dědičnost, protože zavádí možnost, že se vydavatelé a odběratelé budou chovat jinak, v závislosti na tom, ke kterému správci front se připojí. Pokud objekt klastrovaného tématu ponechá libovolné parametry dědit od objektů vyššího tématu, může se toto téma chovat odlišně u různých správců front v daném klastru. Podobně lokálně definované objekty témat definované pod sdruženým objektem tématu ve stromu témat budou znamenat, že tato nižší témata jsou stále klastrovaná, ale lokální objekt může své chování změnit nějakým způsobem, který se liší od ostatních správců front v klastru.

odběry zástupných znaků

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

Pokud se však jiná aplikace přihlašuje k odběru řetězce tématu, který se vyřeší nebo pod tématem klastru, proxy odběry jsou generovány a publikace jsou šířeny do tohoto správce front. Při příchodu originálu je vyšší odběr zástupného znaku považován za oprávněného příjemce těchto publikací a obdrží kopii. Pokud toto chování není povinné, nastavte **`WILDCARD(BLOCK)`** na klastrované téma. 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 dílčích témat.

Související pojmy

Práce s administrativními tématy

Práce s odběry

Související odkazy

ZOBRAZIT TÉMA

ZOBRAZIT STAV TPSTATUS

ZOBRAZIT POD

Atributy tématu klastru

Pokud má objekt tématu nastaven atribut názvu klastru, je definice tématu šířena mezi všemi správci front v klastru. Každý správce front používá šířené atributy témat k řízení chování aplikací typu publikování/odběr.

Objekt tématu má počet atributů, které se používají pro klastry publikování/odběru. Některé řídí obecné chování vydavatelských a odebírajících aplikací a některé řídí, jak je téma používáno v rámci klastru.

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

Například, pokud modelové fronty mají být použity pro spravované odběry (`MDURMDL` a `MNDURMDL`) jsou nastaveny na jiné než výchozí název fronty, tato pojmenovaná modelová fronta musí být definována ve všech správcích front, kde budou vytvořeny spravované odběry.

Podobně, je-li atribut nastaven na hodnotu ASPARENT, bude chování tématu závislé na vyšších uzlech ve stromu témat (viz téma Objekty administrativního tématu). v každém jednotlivém správci front v klastru. To může mít za následek odlišné chování při publikování nebo odběru přihlášení z různých správců front.

Hlavní atributy, které se přímo vztahují k chování publikování/odběru v rámci klastru, jsou následující:

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

- Můžete konfigurovat trasu 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 .
- Když je nastaven parametr **CLUSTER** , nemůžete měnit **CLROUTE** . Chcete-li změnit **CLROUTE**, nejprve nastavte vlastnost **CLUSTER** na prázdnou hodnotu. Tím se zastaví aplikace, které se budou používat v daném tématu klastrovaným způsobem. To způsobí, že dojde k doručení publikování do odběrů, takže byste při provádění této změny měli také uvést systém zpráv publikování/odběru do klidového stavu.

PROXYSUB
Tento parametr řídí, kdy jsou prováděny odběry proxy.

- FIRSTUSE je výchozí hodnota a způsobí odeslání proxy odběrů v odpovědi na lokální odběry ve správci front v distribuované topologii publikování/odběru a zrušení, pokud již není potřeba. Podrobnosti o tom, proč byste mohli chtít změnit tento atribut z výchozí hodnoty FIRSTUSE, najdete v tématu Individuální přesměrování proxy odběru a *publikování všude* .
- Chcete-li povolit *publikování všude*, nastavte parametr **PROXYSUB** na objekt FORCE pro objekt tématu vyšší úrovně. Výsledkem je jednotlivý zástupný odběr se zástupnými znaky, který odpovídá všem tématům pod tímto objektem tématu ve stromu témat.

Poznámka: Nastavení atributu **PROXYSUB(FORCE)** ve velkém nebo ručeném klastru publikování/odběru může mít za následek nadměrné zatížení systémových prostředků. Atribut **PROXYSUB(FORCE)** je šířen do každého správce front, nikoli pouze do správce front, pro kterého bylo téma definováno. To způsobí, že každý správce front v klastru vytvoří zástupný odběr se zástupnými znaky.

Kopie zprávy k tomuto tématu publikovaná v libovolném správci front v klastru je odesílána každému správci front v klastru-buď přímo, nebo prostřednictvím správce front hostitele tématu, v závislosti na nastavení produktu **CLROUTE** .

Je-li téma směrováno přímo, každý správce front vytvoří odesílací kanály klastru pro všechny ostatní správce front. Je-li téma přesměrováno na hostitele témat, jsou kanály pro každého správce front hostitele vytvářeny z každého správce front v daném klastru.

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

PURBOSE a SUBSCOPE
Tyto parametry určují, zda tento správce front šíří publikace do správců front v topologii (klastr nebo klastr systému publikování nebo odběru) nebo omezuje rozsah pouze na jeho lokálního správce front. Ekvivalentní úlohu můžete provést programově pomocí MQPMO_SCOPE_QMGR a MQSO_SCOPE_QMGR.

PUBSCOPE
Je-li objekt tématu klastru definován s produktem **PUBSCOPE(QMGR)**, je definice sdílena s klastrem, ale obor publikování, který je založen na daném tématu, je pouze lokální a neodesílá se do jiných správců front v klastru.

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

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

Nastavení parametru **SUBSCOPE** na hodnotu QMGR v lokální definici tématu nezabrání ostatním správcům front v klastru šíření jejich odběrů proxy do správce front, pokud používají klastrovanou

verzi daného tématu, s produktem **SUBSCOPE(ALL)**. Pokud však lokální definice rovněž nastaví produkt **PUBSCOPE** na hodnotu QMGR , nebudou tyto odběry proxy odeslány z tohoto správce front.

Související pojmy

Obor publikování

Obor odběru

Více definic témat klastru se stejným názvem

Ve více než jednom správci front v klastru můžete definovat stejný pojmenovaný objekt tématu klastru a v určitých scénářích to umožňuje specifické chování. Pokud existuje více definic tématu klastru se stejným názvem, většina vlastností by se měla shodovat. Pokud se nehlásí, vykazují se chyby nebo varování v závislosti na významnosti nesouladu.

Obecně platí, že pokud došlo k neshodě ve vlastnostech více definic témat klastru, jsou vydána varování a jedna z definic objektů tématu je používána každým správcem front v klastru. Která definice je použita každým správcem front, není deterministická nebo konzistentní ve všech správcích front v klastru. Takové neshody by měly být vyřešeny co nejrychleji.

Během nastavování nebo údržby klastru někdy potřebujete vytvořit více definic témat klastru, které nejsou identické. To však platí pouze jako dočasné opatření, a proto se s ním zachází jako s potenciálním chybovým stavem.

Jsou-li zjištěny neshody, jsou do každého protokolu chyb správce front zapsány následující varovné zprávy:

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

Zvolené vlastnosti libovolného řetězce tématu v každém správci front lze určit zobrazením stavu tématu namísto definic témat témat, například pomocí produktu **DISPLAY TPSTATUS**.

V některých situacích je konflikt ve vlastnostech konfigurace dostatečně závažný, aby zastavil vytvářený objekt tématu, nebo aby se neshodující objekty měly označit jako neplatné a nešířeny v klastru (viz **CLSTATE** v DISPLAY TOPIC). K těmto situacím dochází, dojde-li ke konfliktu ve vlastnosti směrování klastru (**CLROUTE**) definic témat. Navíc kvůli důležitosti konzistence mezi různými definicemi směrovaných hostitelů témat jsou další nekonzistence odmítnuty, jak je podrobně popsáno v následujících oddílech tohoto článku.

Je-li konflikt zjištěn v době, kdy je objekt definován, změna konfigurace se odmítne. Pokud je později detekován správci front úplného úložiště, zapíší se do protokolů chyb správců front 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, bude mít lokálně definovaná definice přednost před jakýmkoli vzdáleným definovaným definicí. Proto pokud v definicích existují nějaké rozdíly, správci front, kteří jsou hostiteli více definic, se chovají odlišně.

Efekt pro definování neklastrového tématu se stejným názvem jako téma klastru z jiného správce front

Je možné definovat administrovaný objekt tématu, který není klastrován ve správci front, který se nachází v klastru, a zároveň definuje stejný pojmenovaný objekt tématu jako klastrované definice tématu v jiném správci front. V tomto případě má lokálně definovaný objekt tématu přednost před všemi vzdálenými definicemi stejného názvu.

To má za následek zabránění chování klastrování při použití tohoto tématu 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 matouci chování.

Poznámka: Pokud určitý správce front potřebuje zabránit šíření publikací a odběrů po celém klastru, a to i v případě, že je dané téma klastrováno jinde, může alternativní přístup nastavit obory publikování a odběru pouze na lokálního správce front. Viz “Atributy tématu klastru” na stránce 94.

Více definic témat klastru v klastru s přímým směrováním

Pro přímé směrování obvykle nedefinujete stejné téma klastru ve více než jednom správci front klastru. Důvodem je to, že přímé směrování zpřístupňuje téma u všech správců front v klastru bez ohledu na to, který správce front je definován. Navíc přidání více definic témat klastru významně zvyšuje aktivitu systému a složitost administrativy a se zvyšující se složitostí přichází větší pravděpodobnost lidské chyby:

- Každá definice má za následek přesunutí 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 určit, která definice tématu je používána správcem front.

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

V případě situace, kdy budete možná muset dočasně definovat téma klastru ve druhém správci front, například při odebrání stávajícího hostitele daného tématu z klastru, naleznete informace v tématu Přesun definice tématu klastru do jiného správce front.

Potřebujete-li definici tématu klastru upravit, upravujte ji ve stejném správci front, v němž byla původně definována. Pokus o její úpravu z jiného správce front může náhodně vytvořit druhou definici tématu s konfliktními atributy témat.

Více definic tématu klastru v klastru se směrováním hostitelů témat

Je-li téma klastru definováno s cestou klastru *topic host*, je toto téma šířeno napříč všemi správci front v klastru stejně jako pro *přímá* směrovaná témata. Kromě toho je všem systémem zpráv publikování/odběru pro toto téma směrováno přes správce front, v němž je toto téma definováno. Proto je důležité umístění a počet definic tématu v klastru (viz “Směrování hostitele témat v klastrech publikování/odběru” na stránce 80).

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

Při přidávání nebo odebírání dalších definic směrovacích témat *témat host* v klastru byste měli zvážit tok zpráv v době změny konfigurace. Jsou-li v době změny publikovány zprávy v klastru do tématu změny, je nutný fázovaný proces pro přidání nebo odebrání definice tématu. Přečtěte si téma Přesun definice tématu klastru do jiného správce front a Přidání dalších hostitelů témat do klastru routed hostitelem témat.

Jak již bylo vysvětleno, vlastnosti více definic by měly odpovídat, s možnou výjimkou parametru **PUB** , jak je popsáno v následující sekci. Jsou-li publikace směrovány přes správce front hostitele tématu, je ještě důležitější, aby bylo více definic konzistentní. Proto je nekonzistence zjištěná v řetězci tématu nebo v názvu klastru odmítnuta, pokud byla pro směrování klastru hostitele tématu konfigurována jedna nebo více definic tématu.

Poznámka: Definice témat klastru jsou také odmítnuty, pokud je proveden pokus o jejich konfiguraci nad nebo pod jiným tématem ve stromu témat, kde je existující definice klastrovaného tématu konfigurována pro směrování hostitele témat. Tím se zabrání nejednoznačnosti ve směrování publikací s ohledem na odběry s použitím zástupných znaků.

Speciální zacházení pro parametr PUB

Parametr **PUB** se používá k řízení, kdy lze aplikace publikovat v rámci tématu. V případě směrování hostitele témat v klastru může také určit, které správce front hostitele tématu se používají ke směrování publikací. Z tohoto důvodu je povoleno mít více definic stejného objektu tématu v klastru s různým nastavením pro parametr PUB .

Pokud má více vzdálených klastrovaných definic tématu různá nastavení pro tento parametr, téma umožňuje odeslání a doručení publikací do odběrů, pokud jsou splněny následující podmínky:

- Ve správci front není definován odpovídající objekt tématu, ke kterému je vydavatel připojen, že je nastaven na PUB(DISABLED).
- Jedna nebo více definic více témat v klastru je nastavena na hodnotu PUB(ENABLED) nebo jedna či více definic více témat je nastaveno na PUB(ASPARENT) a lokální správce front, ve kterém je vydavatel připojen, a definované odběry jsou nastaveny na PUB(ENABLED) ve vyšším bodě stromu témat.

Pro směrování hostitele témat jsou zprávy, které jsou publikovány aplikacemi připojenými ke správcům front, které nejsou hostiteli témat, směrovány pouze na téma hostování správců front, kde parametr **PUB** nebyl explicitně nastaven na hodnotu DISABLED. Můžete proto použít nastavení PUB(DISABLED) pro uvedení provozu zpráv do klidového stavu pomocí určitých hostitelů témat. Můžete to chtít provést pro přípravu na údržbu nebo odebrání správce front nebo z důvodů popsaných v tématu Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu.

Dostupnost správců front hostitele tématu klastru
Navrhněte klastr publikování/odběru, abyste minimalizovali riziko, že by se správce front hostitele tématu stal nedostupným, klastr již nebude schopen zpracovat provoz pro dané téma. Vliv správce front hostitele tématu, který se stává nedostupným, závisí na tom, zda klastr používá směrování hostitele témat nebo přímé směrování.

Dostupnost správců front hostitele tématu, kteří používají přímé směrování

Pro přímé směrování obvykle nedefinujete stejné téma klastru ve více než jednom správci front klastru. Důvodem je to, že přímé směrování zpřístupňuje téma u všech správců front v klastru bez ohledu na to, který správce front je definován.Viz téma Několik definic témat klastru v klastru s přímým směrováním.

Kdykoli v klastru dojde k nedostupnosti hostitele klastrovaného objektu (například klastrované fronty nebo klastrované téma) po delší dobu, ostatní členové klastru nakonec ukončí platnost znalosti těchto objektů. V případě klastrovaného tématu, je-li správce front hostitele tématu klastru nedostupný, budou ostatní správci front nadále zpracovávat požadavky na publikování/odběr pro dané téma v přímé klastrované cestě (tedy odesílání publikování na odběry u vzdálených správců front) po dobu nejméně 60 dnů od okamžiku, kdy byl správce front tématu naposledy v komunikaci se správci front úplného úložiště. Je-li správce front, ve kterém jste definovali objekt tématu klastru, nikdy znovu k dispozici, budou odstraněny objekty témat uložené v mezipaměti v jiných správcích front a téma se vrátí k lokálnímu tématu, kdy odběry z aplikací připojených ke vzdáleným správcům front přestanou přijímat publikování.

Při 60 dnech pro zotavení správce front, ve kterém definujete objekt tématu klastru, je třeba věnovat zvláštní pozornost tomu, aby bylo zaručeno, že hostitel tématu klastru zůstane dostupný (všimněte si však, že žádné odběry definované na nedostupném hostiteli tématu klastru nebudou k dispozici). Lhůta 60 dnů postačuje k zajištění technických problémů a pravděpodobně dojde k překročení pouze kvůli problémům s administrativními chybami. Chcete-li tuto možnost zmírnit, pokud hostitel tématu klastru není k dispozici, všichni členové zprávy protokolu chyb zápisu klastru budou mít hodinu zprávy o tom, že příslušný objekt tématu klastru uložený v mezipaměti nebyl aktualizován. Reagujte na tyto zprávy a ujistěte se, že správce front, na kterém je definován objekt tématu klastru, je spuštěn. Pokud není možné znovu zpřístupnit správce front hostitele tématu klastru, definujte stejnou definici klastrovaného tématu s přesně stejnými atributy u jiného správce front v klastru.

Dostupnost správců front hostitele témat, kteří používají směrování hostitele témat

Pro směrování hostitele témat je všem systému zpráv publikování/odběru pro dané téma směrováno přes správce front, v němž je toto téma definováno. Z tohoto důvodu je velmi důležité brát v úvahu nepřetržitou

dostupnost těchto správců front v klastru. Pokud se hostitel tématu stane nedostupným a pro dané téma neexistuje žádný jiný hostitel, přenos od vydavatelů k odběratelům v různých správcích front v klastru se pro dané téma okamžitě zastaví. Jsou-li k dispozici další hostitelé témat, bude správce front klastru směrovat nový publikační provoz prostřednictvím těchto hostitelů témat a poskytovat tak průběžnou dostupnost tras zpráv.

Co se týče přímých témat, po 60 dnech, je-li první hostitel tématu stále nedostupný, je z klastru odebráno informace o tématu hostitele daného tématu. Jedná-li se o poslední zbývající definici tohoto tématu v klastru, všichni ostatní správci front přestanou předávat publikace všem hostitelům témat ke směrování.

Chcete-li zajistit odpovídající dostupnost a rozšiřitelnost, je tedy užitečné, pokud možno, definovat každé téma alespoň na dvou správcích front klastru. To poskytuje ochranu proti kterému správci front hostitele tématu, které se stanou nedostupnými. Viz také téma Několik definic tématu klastru v klastru se směrováním hostitele témat.

Pokud nemůžete konfigurovat více hostitelů témat (například proto, že potřebujete zachovat řazení zpráv) a nemůžete nakonfigurovat pouze jednoho hostitele tématu (protože dostupnost jednoho správce front nesmí ovlivnit tok publikací do odběrů u všech správců front v klastru), zvažte možnost konfigurace tématu jako tématu s přímým směrováním. Tím se vyvarujete závislosti na jednom správci front pro celý klastr, ale stále vyžaduje, aby byl každý jednotlivý správce front k dispozici, aby mohl zpracovávat lokálně hostované odběry a vydavatele.

Blokující publish/odběr v klastru

Představení první přímé směrované klastrované téma do klastru vynutí, aby každý správce front v klastru byl informován o všech ostatních správci front, a potenciálně tak může způsobit vytvoření kanálů. Pokud to není žádoucí, měli byste místo toho nakonfigurovat publish/subscribe hostitele tématu. Pokud by existence klastru s přímým směrováním mohla ohrozit stabilitu klastru kvůli škálování obav každého správce front, můžete zcela vypnout funkce klastrovaných publikování/odběru nastavením **PSCLUS** na hodnotu DISABLED na každém správci front v klastru.

Jak je popsáno v tématu“Přímé směrování v klastrech publikování/odběru” na stránce 75, když představujete klastrované téma s přímým směrováním do klastru, všechna dílčí úložiště jsou automaticky upozorněna na všechny ostatní členy klastru. Klastrované téma může také vytvořit odběry ve všech ostatních uzlech (například tam, kde je zadáno **PROXYSUB(FORCE)**) a způsobit spuštění velkého počtu kanálů ze správce front, a to i v případě, že neexistují lokální odběry. To znamená okamžité další načtení pro každého správce front v klastru. V případě klastru, který obsahuje mnoho správců front, může dojít k výraznému snížení výkonu. Proto je třeba pečlivě naplánovat zavedení přímého přesměrovaného publikování/odběru klastru do klastru.

Když víte, že klastr nemůže pojmout režijní náklady přímého přesměrovaného publikování/odběru, můžete místo toho použít publish/subscribe hostované hostitele tématu. Přehled rozdílů viz “Návrh klastrů publikování a odběru” na stránce 73.

Dáváte-li přednost zcela znepřístupnění funkcí publikování/odběru pro daný klastr, můžete tak učinit nastavením atributu správce front **PSCLUS** na hodnotu DISABLED na každém správci front v daném klastru. Toto nastavení zakazuje přímé přesměrování publikování a přihlášení hostitele do klastru tím, že upraví tři aspekty funkcí správce front:

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

Ačkoli **PSCLUS** je parametrem každého jednotlivého správce front v klastru, není zamýšlen selektivně zakázat publikování/odběr v podmnožině správců front v klastru. Pokud je tímto způsobem vypnuto, zobrazí se časté chybové zprávy. Je tomu tak proto, že proxy odběry a definice témat se neustále zobrazují a jsou odmítány, je-li téma klastrovat na správci front, kde je produkt **PSCLUS** povolen.

Měli byste se proto zaměřit na nastavení **PSCLUS** na DISABLED na každém správci front v klastru. V praxi se však může stát, že tento stav může být obtížné dosáhnout a udržovat, například správci front se mohou

připojit a ponechat klastr kdykoli. Přinejmenším je třeba zajistit, aby byl produkt **PSCLUS** nastaven na hodnotu DISABLED ve všech správcích front úplného úložiště. Pokud tak učiníte a klastrované téma je následně definováno na správci front ENABLED v klastru, nezpůsobí to úplná úložiště, která by informovala každého správce front o každém jiném správci front, a proto je váš klastr chráněn před potenciálními problémy se škálováním pro všechny správce front. V tomto scénáři je původ klastrovaného tématu hlášen v protokolech chyb správců front úplného úložiště.

Pokud se správce front podílí na jednom nebo více klastrech publikování/odběru, a také jeden nebo více klastrů typu point-to-point, musíte v tomto správci front nastavit parametr **PSCLUS** na hodnotu ENABLED . Z tohoto důvodu byste měli při překrývání klastru mezi dvěma body a klastru s publikačním odběrem použít samostatnou sadu úplných úložišť v každém klastru. Tento přístup umožňuje definovat definice témat a informace o každém správci front pouze v klastru publikování/odběru.

Chcete-li se vyhnout nekonzistentním konfiguracím, když změníte **PSCLUS** z ENABLED na DISABLED, žádné klastrované objekty témat nemohou existovat v žádném klastru, jehož je tento správce front členem. Všechna taková témata, a to i vzdáleně definovaná, musí být odstraněna před změnou **PSCLUS** na DISABLED.

Další informace o produktu **PSCLUS**naleznete v tématu ALTER QMGR (PSCLUS).

Související pojmy

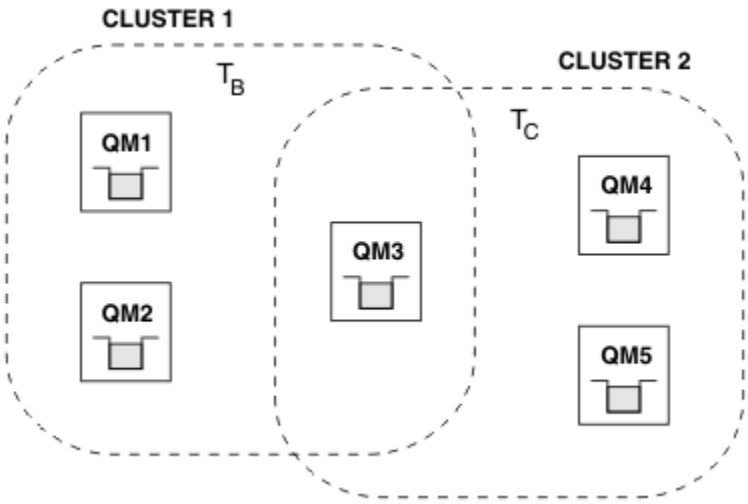
Výkon klastru přímého nasměrování publikování/odběru

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 a odběru” na stránce 73.

Aspekty návrhu pro zachovaná publikování v klastrech publikování/odběru

Při návrhu klastru publikování/odběru pro práci se zachovaným publikováním je třeba vzít v úvahu několik omezení.

Podmínky

Úvaha 1: Následující správci front klastru vždy ukládají nejnovější verzi zachovaného publikování:

- Správce front vydavatele
- V hostovaném klastru hostitele tématu (za předpokladu, že existuje pouze jeden hostitel tématu pro dané téma, jak je vysvětleno v následující části tohoto článku).
- Všichni správci front s odběry shodujících se s řetězcem tématu zachovaného publikování

Rozhodnutí 2: Správci front se nepřijímají aktualizované zachované publikace, zatímco nemají žádné odběry. Všechny zachované publikování uložené ve správci front, které již není přihlášeno k odběru tématu, se stane zastaralým.

Pokyn 3: Při vytváření libovolného odběru, pokud existuje lokální kopie zachovaného publikování pro řetězec tématu, je lokální kopie doručena do odběru. Jste-li prvním odběratelem pro libovolný řetězec tématu, bude z jednoho z následujících členů klastru doručeno i odpovídající zachované publikování:

- V přímo směrovém klastru, správce front vydavatele
- V klastru se směrováním hostitele témat jsou hostitelé témat 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 zachovaná publikace vynechána až do dalšího volání do produktu `MQSUBRQ`.

Důsledky

U každého klastru publikování/odběru, je-li proveden první odběr, může lokální správce front uložit zastaralou kopii zachovaného publikování a toto je kopie, která je doručena novému odběru. Existence odběru u lokálního správce front znamená, že se tento stav vyřeší při příští aktualizaci zachovaného publikování.

Pokud v případě klastru publikování/odběru pro daný uzel konfigurujete více než jednoho hostitele témat pro dané téma, mohou noví odběratelé obdržet nejnovější zachované publikování od hostitele tématu nebo mohou obdržet zastaralé zachované publikování z jiného hostitele tématu (s poslední ztrátou). Pro směrování hostitele témat je obvyklé konfigurovat více hostitelů témat pro dané téma. Pokud však očekáváte, že aplikace budou používat zachovaná publikování, měli byste pro každé téma nakonfigurovat pouze jednoho hostitele témat.

Pro každý zadaný řetězec tématu byste měli používat pouze jednoho vydavatele a zajistit, že vydavatel vždy používá stejného správce front. Pokud tuto akci neuděláte, mohou být v různých správcích front pro stejné téma aktivní jiné zachované publikace, což vede k neočekávanému chování. Vzhledem k tomu, že je distribuován více odběrů proxy, může být přijato více zachovaných publikování.

Pokud se stále více zajímají o odběratele používající zastaralé publikace, zvažte nastavení vypršení platnosti zprávy při vytváření jednotlivých zachovaných publikování.

Chcete-li odebrat zachované publikování z klastru publikování/odběru, můžete použít příkaz **CLEAR TOPICSTR** . Za určitých okolností může být nutné zadat příkaz na více členech klastru publikování/odběru, jak je popsáno v tématu **CLEAR TOPICSTR** .

Použití zástupných znaků a zachovaných publikování

Pokud používáte zástupné znaky odběrů, jsou odpovídající odběry proxy doručené ostatním členům klastru publikování/odběru zástupné znaky z oddělovače témat bezprostředně před prvním zástupným znakem. Viz Zástupné znaky a témata klastru.

Proto může použitý zástupný znak odpovídat více řetězcům témat a více zachovaným publikacím, než se bude shodovat s odběratelské aplikací.

Tím se zvyšuje množství úložného prostoru potřebného pro zachované publikace, a proto je třeba zajistit, aby hostující správci front měli dostatečnou kapacitu pro ukládání dat.

Související pojmy

Zachovaná publikování

Přesílání jednotlivých odběrů proxy a publikování všude

Aspekty REFRESH CLUSTER pro klastry publikování/odběru

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

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

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

Narušení klastru se může objevit zvnějšku jako tyto symptomy:

- Odběry témat klastru v tomto správci front nepřijímají publikování od vydavatelů, kteří jsou připojeni k jiným správcům front v klastru.
- Zprávy publikované v rámci témat klastru v tomto správci front nejsou šířeny do odběrů u jiných správců front.
- Odběry témat klastru na tomto správci front vytvořené během tohoto období nekonzistentně odesílají proxy odběry do jiných členů klastru.
- Odběry témat klastru na tomto správci front, které byly odstraněny během tohoto období, nejsou konzistentně odebírající proxy odběry z jiných členů klastru.
- 10-sekundové pauzy, nebo delší, při doručování zpráv.

- Selhání produktu **MQPUT** , například MQRC_PUBLICATION_FAILURE.
- Publikace umístěné ve frontě nedoručených zpráv s příčinou MQRC_UNKNOWN_REMOTE_Q_MGR

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

Po zadání příkazu **REFRESH CLUSTER** u správce front v klastru pro publikování/odběr počkejte, dokud nebudou úspěšně obnoveny všechny správce front klastru a témata klastru a poté proveďte opětovnou synchronizaci proxy odběrů, jak je popsáno v tématu Resynchronizace odběrů proxy. Pokud byly všechny odběry proxy správně synchronizovány, restartujte aplikace publikování/odběru.

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

Související pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 67

Příkaz **REFRESH CLUSTER** se používá k zahození všech lokálně uložených informací o klastru a znovusestavení těchto informací z úplných úložišť v klastru. Tento příkaz byste neměli používat, kromě výjimečných okolností. Pokud ji potřebujete použít, musíte zvážit, jak ji budete používat. Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

Problémy aplikace zaznamenané při spuštění REFRESH CLUSTER

Související odkazy

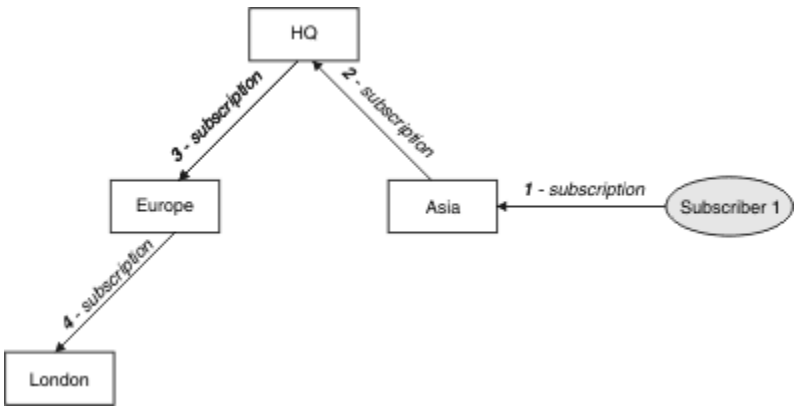
Popis příkazů MQSC: REFRESH CLUSTER

Směrování v hierarchiích publikování/odběru

Je-li distribuovaná topologie správce front nastavena na hierarchii publikování/odběru a odběr je proveden ve správci front, dojde při výchozím nastavení k vytvoření odběru serveru proxy pro všechny správce front v hierarchii. Příručky přijaté na libovolném správci front jsou poté směrovány přes hierarchii ke každému správci front, který je hostitelem odpovídajícího odběru.

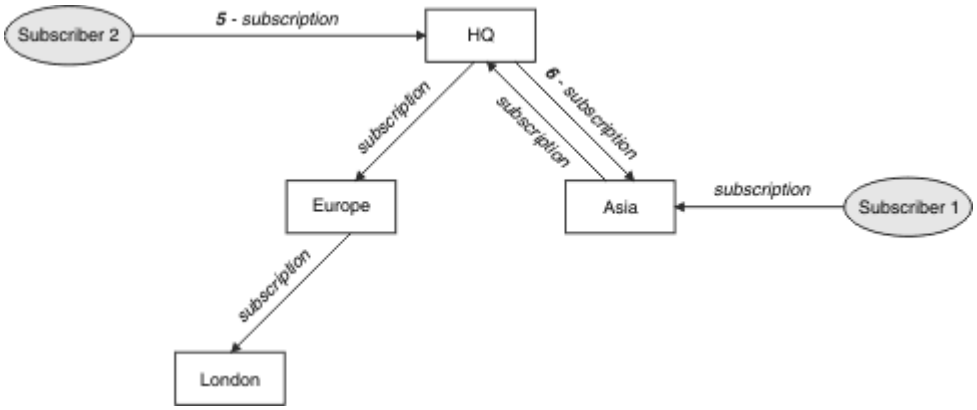
Úvod do způsobu, jakým jsou zprávy směrovány mezi správci front v hierarchiích publikování a odběru a v klastrech, najdete v tématu Distribuované sítě typu publikování/odběr.

Je-li odběr tématu proveden ve správci front v rámci distribuované hierarchie publikování/odběru, spravuje správce front proces, při kterém je odběr šířen do připojených správců front. *Proxy odběry* proudí do všech správců front v síti. Proxy odběr poskytuje správci front informace, které potřebuje k předání publikování těm správcům front, kteří jsou hostiteli odběrů daného tématu. Každý správce front v hierarchii publikování/odběru je informován pouze o svých přímých vztazích. Publikování odeslaná do jednoho správce front jsou prostřednictvím svých přímých vztahů odesílány k těmto správcům front s odběry. Toto je znázorněno na následujícím obrázku, ve kterém *Odběratel 1* registruje odběr pro konkrétní téma ve správci front *Asia* (1). Proxy odběry pro tento odběr na správci front *Asia* jsou předány všem ostatním správcům front v síti (2,3, 4).



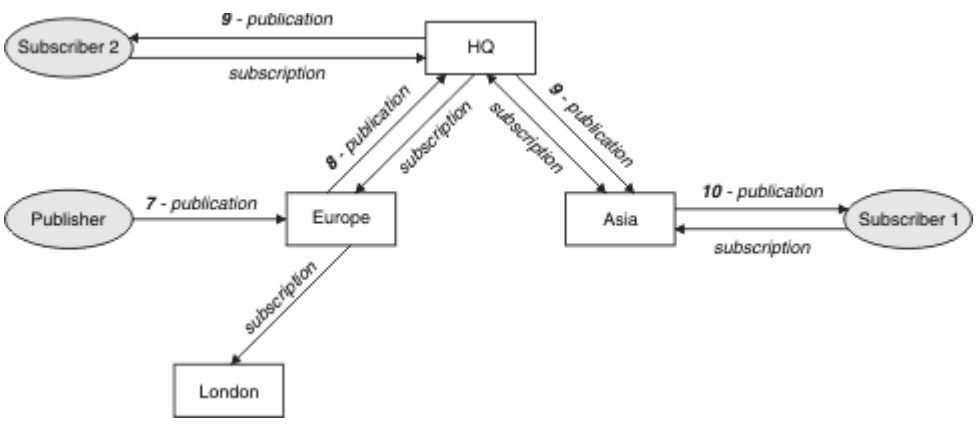
Obrázek 29. Šíření odběrů prostřednictvím sítě správce front

Správce front konsoliduje všechny odběry, které jsou v ní vytvořeny, ať už z lokálních aplikací, nebo ze vzdálených správců front. Vytvoří proxy odběry pro témata odběrů se svými sousedy, pokud proxy odběr již neexistuje. To je ilustrováno na následujícím obrázku, ve kterém *Odběratel 2* registruje odběr na stejné téma jako v produktu Obrázek 29 na stránce 103ve správci front *HQ* (5). Odběr pro toto téma je předáván správci front *Asia* , takže si je vědom toho, že odběry existují i jinde v síti (6). Odběr není přesměrován do správce front *Europe* , protože odběr pro toto téma již byl zaregistrován; viz krok 3 v příručce Obrázek 29 na stránce 103.



Obrázek 30. Více odběrů

Když aplikace publikuje informace do určitého tématu, předávající správce front ji předá všem správcům front, kteří mají platné odběry tématu. Může ji předávat prostřednictvím jednoho nebo více zprostředkujících správců front. To je ilustrováno na následujícím obrázku, v němž vydavatel odešle publikování ve stejném tématu jako v produktu Obrázek 30 na stránce 104do správce front *Europe* (7). Odběr pro toto téma existuje z *HQ* do *Europe*, takže je publikace předána do správce front *HQ* (8). Neexistuje však žádný odběr z *Londýna* do *Evropy* (pouze z *Evropy* do *London*), takže publikování není přesměrováno na správce front *London* . Správce front *HQ* odešle publikaci přímo do objektu *Subscriber 2* a do správce front *Asia* (9). Publikace je předávána *Subscriber 1* from *Asia* (10).



Obrázek 31. Šíření publikací prostřednictvím sítě správce front

Odešle-li správce front do jiného správce front publikace nebo odběry, nastaví vlastní ID uživatele ve zprávě. Pokud používáte hierarchii publikování/odběru, a pokud je příchozí kanál nastaven tak, aby odesílal zprávy s oprávněním ID uživatele ve zprávě, musíte autorizovat ID uživatele odesílajícího správce front. Viz téma Použití výchozích uživatelských jmen s hierarchií správce front.

Poznámka: Pokud místo toho použijete klastry typu publikování-odběr, bude autorizace zpracována klastrem.

Souhrn a další pokyny

Hierarchie publikování/odběru vám poskytuje přesnou kontrolu nad vztahem mezi správci front. Po jeho vytvoření potřebuje malý ruční zásah k administrativu. Uvede však také určitá omezení na vašem systému:

- Vyšší uzly v hierarchii, zejména kořenový uzel, musí být hostovány na robustních, vysoce dostupných a výkonnostních zařízeních. Důvodem je to, že se očekává, že provoz těchto uzlů bude procházet více publikačních přenosů.
- Dostupnost všech nelistových správců front v hierarchii ovlivňuje schopnost sítě směrovat zprávy od vydavatelů k odběratelům v jiných správcích front.
- Ve výchozím nastavení jsou všechny řetězce témat přihlášené k odběru šířeny v rámci hierarchie a publikace jsou šířeny pouze pro vzdálené správce front, kteří mají odběr k přidruženému tématu. Proto se rychlé změny souboru odběrů mohou stát limitujícím faktorem. Toto výchozí chování můžete změnit a místo toho budou všechny publikace šířeny pro všechny správce front, čímž dojde k odebrání nutnosti proxy odběrů. Viz téma Výkon odběru v sítích typu publikování/odběr.

  Poznámka: Obdobná omezení platí i pro přímé směrované klastry.
- Vzhledem k propojené povaze správců front publikování/odběru je třeba, aby se proxy odběry rozšířily na všechny uzly v síti. Vzdálené publikace nemusí být nutně odebírané okamžitě, takže časné publikace nemusí být odeslány na základě odběru nového řetězce tématu. Problémy způsobené prodlevou odběru můžete odstranit tím, že budou všechny publikace šířeny pro všechny správce front, což odstraňuje nutnost proxy odběrů. Viz téma Výkon odběru v sítích typu publikování/odběr.

  Poznámka: Toto omezení platí také pro přímé směrované klastry.
- Pro hierarchii publikování/odběru, přidání nebo odebrání správců front vyžaduje ruční konfiguraci do hierarchie, s pečlivým zvážením umístění těchto správců front a jejich závislostí na jiných správcích front. Pokud nepřidáváte nebo neodebíráte správce front, kteří jsou ve spodní části hierarchie, a tudíž nemají žádné další větve pod nimi, budete také muset konfigurovat ostatní správce front v hierarchii.

Před použitím hierarchie publikování/odběru jako mechanismu směrování prozkoumejte alternativní přístupy podrobně popsané v části “Přímé směrování v klastrech publikování/odběru” na stránce 75 a “Směrování hostitele témat v klastrech publikování/odběru” na stránce 80.

Systémové fronty distribuovaného publikování/odběru

Správci front pro systém zpráv publikování/odběru používají čtyři systémové fronty. Musíte si být vědomi své existence pouze pro účely určování problémů a plánování kapacity.

Informace o tom, jak monitorovat tyto fronty, najdete v tématu Vyvážení výrobců a odběratelů v sítích publikování/odběru .

Tabulka 6. Systémové fronty publikování/odběru v rámci platformy Multiplatforms

Systémová fronta	**Účel**
SYSTEM.INTER.QMGR.CONTROL	IBM MQ distribuovaná řídicí fronta publikování/odběru
SYSTEM.INTER.QMGR.FANREQ	IBM MQ distribuovaná fandová vstupní fronta procesu větvení proxy odběru publikování/odběru
SYSTEM.INTER.QMGR.PUBS	Publikace IBM MQ distribuovaných publikování/odběru
SYSTEM.HIERARCHY.STATE	Stav relace hierarchie distribuovaného publikování/odběru IBM MQ

z/OS V systému z/OSnastavíte při vytváření správce front potřebné systémové objekty, a to včetně ukázek CSQ4INSX, CSQ4INSR a CSQ4INSG ve vstupní datové sadě inicializace CSQINP2 . Další informace naleznete v tématu Úloha 13: Úprava vstupních datových sad inicializace.

Atributy systémových front publikování/odběru jsou zobrazeny v Tabulka 7 na stránce 106.

Tabulka 7. Atributy front systému publikování/odběru	
Atribut	**Výchozí hodnota**
DEFPSIST	Ano
DEFSOPT	SHARED
MAXMSGL	Multi V systému Multiplatforms: Hodnota parametru MAXMSGL příkazu ALTER QMGR z/OS V 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: Jediná fronta, která obsahuje zprávy odeslané aplikacemi, je `SYSTEM.INTER.QMGR.PUBS`. **MAXDEPTH** je nastaven na svou maximální hodnotu pro tuto frontu, aby bylo povoleno dočasné sestavení publikovaných zpráv během výpadků nebo při překročení příliš vysoké zátěže. Je-li správce front spuštěn v systému, kde nebyla obsažena tato hloubka fronty, mělo by být toto nastavení upraveno.

Související úlohy

Odstraňování problémů distribuovaného publikování/odběru

Chyby fronty distribuovaného publikování/odběru zpráv

Chyby se mohou vyskytnout, když jsou distribuované fronty správce front publikování/odběru nedostupné. To má vliv na šíření znalostí odběru v síti publikování/odběru a publikování na odběry vzdálených správců front.

Je-li fronta požadavků na výstupní větvení `SYSTEM.INTER.QMGR.FANREQ` nedostupná, vytvoření odběru může generovat chybu a chybové zprávy budou zapsány do protokolu chyb správce front, pokud je nutné doručit proxy odběry přímo připojeným správcům front.

Pokud je fronta stavu relace s hierarchií `SYSTEM.HIERARCHY.STATE` nedostupná, zapíše se do protokolu chyb správce front chybová zpráva a do režimu produktu `COMPAT` se vloží stroj publikování/odběru. Chcete-li zobrazit režim publikování/odběru, použijte příkaz `DISPLAY QMGR PSMODE`.

Pokud nejsou k dispozici žádné jiné fronty produktu `SYSTEM.INTER.QMGR` , je do protokolu chyb správce front zapsána chybová zpráva a přestože funkce není zakázána, je pravděpodobné, že zprávy publikování/odběru budou ve frontách na těchto nebo vzdálených správcích front sestavovat fronty.

Je-li fronta systému publikování/odběru nebo požadovaná přenosová fronta do nadřízeného, podřízeného nebo publikovaného/subscribového správce front klastru nedostupná, dojde k následujícím výsledkům:

- Publikace nejsou doručeny a publikační aplikace může obdržet chybu. Podrobnosti o tom, kdy publikující aplikace obdrží chybu, naleznete v následujících parametrech příkazu **DEFINE TOPIC** : **PMSGDLV** , **NPMSGDLV** a **USEDLQ** .
- Přijaté publikace mezi správci front se zálohují do vstupní fronty a následně se o ně znovu pokusili. Je-li dosažen práh vrácení, jsou nedoručené publikace umístěny do fronty nedoručených zpráv. Protokol chyb správce front bude obsahovat podrobnosti o problému.
- Nedoručený odběr serveru proxy se odzálohuje do fronty požadavků výstupního větvení a následně se pokusí o další pokus. Je-li dosažena prahová hodnota vrácení, nedoručitelná proxy odběr není doručena žádnému propojenému správci front a bude umístěna do fronty nedoručených zpráv. Protokol chyb správce front bude obsahovat podrobnosti o problému včetně podrobností o nezbytných nezbytných opravných administračních akcích.

- Zprávy protokolu relace hierarchie se nezdařily a stav připojení je označen jako ERR0R. Chcete-li zobrazit stav připojení, použijte příkaz **DISPLAY PUBSUB**.

Související úlohy

Odstraňování problémů distribuovaného publikování/odběru

Multi Plánování systémů pro ukládání dat a výkonu na platformách Multiplatforms

Musíte nastavit realistické a dosažitelné úložiště a výkonnostní cíle pro váš systém IBM MQ . Použijte odkazy k vyhledání informací o faktorech, které ovlivňují úložiště a výkon na platformě.

Požadavky se liší v závislosti na systémech, na kterých používáte produkt IBM MQ , a které komponenty chcete použít.

Nejnovější informace o podporovaných hardwarových a softwarových prostředích najdete v tématu Systémové požadavky pro IBM MQ.

Produkt IBM MQ ukládá data správce front do systému souborů. Použijte následující odkazy, abyste zjistili informace o plánování a konfiguraci adresářových struktur pro použití s produktem IBM MQ:

- “Plánování podpory systému souborů na více platformách” na stránce 111
- “Požadavky na sdílené systémy souborů na platformě Multiplatforms” na stránce 112
- “Sdílení souborů IBM MQ na platformách Multiplatforms” na stránce 121
- Linux AIX “Adresářová struktura v systémech AIX and Linux” na stránce 124
- Windows “Adresářová struktura v systémech Windows” na stránce 133
- IBM i “Adresářová struktura v systému IBM i” na stránce 136

Použijte následující odkazy pro informace o systémových prostředcích, sdílené paměti a priority procesů na serveru AIX and Linux:

- Linux AIX “Zdroje pro produkt IBM MQ a UNIX System V IPC” na stránce 141
- AIX “Sdílená paměť v systému AIX” na stránce 140
- Linux AIX “Priorita procesu IBM MQ a UNIX” na stránce 141

Pro informace o souborech protokolu použijte následující odkazy:

- “Výběr kruhového nebo lineárního protokolování na více platformách” na stránce 139
- Výpočet velikosti protokolu

Související pojmy

“Plánování vašeho prostředí IBM MQ na systému z/OS” na stránce 141
Při plánování vašeho prostředí IBM MQ musíte vzít v úvahu požadavky na prostředky pro datové sady, sady stránek, Db2, Prostředky párování a potřebu protokolování a zálohování zařízení. Pomocí tohoto tématu můžete naplánovat prostředí, ve kterém 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

Požadavky na hardware a software v systému AIX and Linux

Požadavky na hardware a software v systému Windows

Multi Požadavky na prostor na disku na platformách

Požadavky na úložný prostor produktu IBM MQ závisí na tom, které komponenty instalujete a kolik pracovního prostoru budete potřebovat.

Diskové úložiště se požaduje pro volitelné komponenty, které se rozhodnete instalovat, včetně všech požadovaných komponent, které vyžadují. Požadavek na celkové úložiště závisí také na počtu používaných front, počtu a velikosti zpráv ve frontách a na tom, zda jsou zprávy trvalé. Požadujete také archivační kapacity na disku, pásce nebo jiném médiu, stejně jako prostor pro vaše vlastní aplikační programy.

Následující tabulky zobrazují přibližný prostor na disku požadovaný při instalaci různých kombinací produktu na různých platformách. (Hodnoty se zaokrouhlují nahoru na nejbližší 5 MB, kde je MB 1 048 576 bajtů.)

- LTS "Požadavky na prostor na disku pro Long Term Support" na stránce 108
- CD "Požadavky na prostor na disku pro Continuous Delivery" na stránce 109

Požadavky na prostor na disku pro Long Term Support

LTS V 9.2.0

Tabulka 8. IBM MQ disk space requirements for 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	325 MB	370 MB	1690 MB
IBM i IBM i (viz Další poznámky pro systém IBM i)	480 MB	840 MB	1815 MB
Linux Linux for x86-64	245 MB	270 MB	1835 MB
Linux Linux on POWER Systems - Little Endian	150 MB	170 MB	1205 MB
Linux Linux for IBM Z	235 MB	260 MB	1240 MB
Windows Windows (64bitová instalace) "4" na stránce 109	280 MB	390 MB	1755 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 v systémech Windows ; jejich funkčnost je někdy zahrnuta do jiných funkcí. Viz téma Funkce produktuIBM MQ pro systémy Windows.

Další poznámky pro systém IBM i: IBM i

1. V systému IBM i nelze oddělit nativního klienta od serveru. Číslo serveru v tabulce je určeno pro 5724H72*BASE bez Java, spolu s Anglickou jazykovou zátěží (2924). Existuje 22 možných jedinečných jazykových zátěží.
2. Obrázek v tabulce je určen pro nativního klienta 5725A49 *BASE bez Java.
3. Třídy Java a JMS lze přidat k vazbám 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 prostor na disku pro Continuous Delivery

CD

Tabulka 9. IBM MQ disk space requirements for Multiplatforms for Continuous Delivery

Verze Platform/CD	Instalace klienta "1" na stránce 111	Instalace serveru "2" na stránce 111	Úplná instalace "3" na stránce 111
AIX **AIX**			
V 9.2.0 IBM MQ 9.2.0	150 MB	205 MB	1410 MB
V 9.2.1 IBM MQ 9.2.1	325 MB	370 MB	1690 MB
V 9.2.2 IBM MQ 9.2.2	325 MB	370 MB	1690 MB
V 9.2.3 IBM MQ 9.2.3	325 MB	370 MB	1690 MB
V 9.2.4 IBM MQ 9.2.4	330 MB	375 MB	1690 MB
V 9.2.5 IBM MQ 9.2.5	330 MB	375 MB	1760 MB
Linux **Linux for x86-64 (64 bitů)**			
V 9.2.0 IBM MQ 9.2.0	130 MB	185 MB	1645 MB
V 9.2.1 IBM MQ 9.2.1	245 MB	270 MB	1835 MB
V 9.2.2 IBM MQ 9.2.2	245 MB	270 MB	1835 MB
V 9.2.3 IBM MQ 9.2.3	245 MB	270 MB	1835 MB

Tabulka 9. IBM MQ disk space requirements for Multiplatforms for Continuous Delivery (pokračování)			
Verze Platform/CD	**Instalace klienta** **"1" na stránce 111**	**Instalace serveru** **"2" na stránce 111**	**Úplná instalace** **"3" na stránce 111**
V 9.2.4 IBM MQ 9.2.4	245 MB	270 MB	1870 MB
V 9.2.5 IBM MQ 9.2.5	265 MB	295 MB	2010 MB
Linux **Linux on POWER Systems - Little Endian**			
V 9.2.0 IBM MQ 9.2.0	95 MB	135 MB	1100 MB
V 9.2.1 IBM MQ 9.2.1	150 MB	170 MB	1205 MB
V 9.2.2 IBM MQ 9.2.2	150 MB	170 MB	1205 MB
V 9.2.3 IBM MQ 9.2.3	150 MB	170 MB	1205 MB
V 9.2.4 IBM MQ 9.2.4	150 MB	170 MB	1210 MB
V 9.2.5 IBM MQ 9.2.5	170 MB	190 MB	1350 MB
Linux **Linux pro IBM Z**			
V 9.2.0 IBM MQ 9.2.0	130 MB	175 MB	1130 MB
V 9.2.1 IBM MQ 9.2.1	235 MB	265 MB	1255 MB
V 9.2.2 IBM MQ 9.2.2	235 MB	265 MB	1255 MB
V 9.2.3 IBM MQ 9.2.3	235 MB	265 MB	1255 MB
V 9.2.4 IBM MQ 9.2.4	235 MB	265 MB	1300 MB
V 9.2.5 IBM MQ 9.2.5	255 MB	290 MB	1435 MB
Windows **Windows (64bitová instalace)** "4" na stránce 111			
V 9.2.0 IBM MQ 9.2.0	230 MB	365 MB	1565 MB

Tabulka 9. IBM MQ disk space requirements for Multiplatforms for Continuous Delivery (pokračování)			
Verze Platform/CD	**Instalace klienta** “1” na stránce 111	**Instalace serveru** “2” na stránce 111	**Úplná instalace** “3” na stránce 111
V 9.2.1 IBM MQ 9.2.1	280 MB	390 MB	1900 MB
V 9.2.2 IBM MQ 9.2.2	280 MB	390 MB	1900 MB
V 9.2.3 IBM MQ 9.2.3	280 MB	390 MB	1900 MB
V 9.2.4 IBM MQ 9.2.4	280 MB	390 MB	1950 MB
V 9.2.5 IBM MQ 9.2.5	290 MB	410 MB	2095 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 v systémech Windows ; jejich funkčnost je někdy zahrnuta do jiných funkcí. Viz téma Funkce produktuIBM MQ pro systémy Windows.

Související pojmy

Komponenty a funkce produktu IBM MQ

Multi Plánování podpory systému souborů na více platformách

Data správce front jsou uložena v systému souborů. Správce front využívá zamykání systému souborů k zabránění, aby více instancí správce front s více instancemi bylo současně aktivních.

Sdílené systémy souborů

Sdílené systémy souborů umožňují současně přistupovat k jednomu fyzickému úložnému zařízení více systémů. K poškození může dojít v případě, že více systémů přistupuje ke stejnému fyzickému úložnému zařízení přímo, aniž by došlo k vynucnutí blokování a řízení souběžnosti. Operační systémy poskytují lokální systémy souborů s uzamčením a řízením souběžnosti pro lokální procesy; síťové systémy souborů poskytují zamykání a řízení souběžnosti pro distribuované systémy.

Historicky nebyly síťové systémy souborů prováděny dostatečně rychle nebo poskytly dostatečné uzamčení a řízení souběžnosti, aby splňovaly požadavky na protokolování zpráv. Dnes mohou síťové systémy souborů zajistit dobrou výkonnost a implementace spolehlivých protokolů síťového systému souborů, jako například *RFC 3530, Network File System (NFS) verze 4 protocol*, splňují požadavky na spolehlivé protokolování zpráv.

Sdílené systémy souborů a 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 správce front a soubory protokolu umístěny ve sdíleném síťovém systému souborů. IBM i V IBM ise používají žurnály místo souborů protokolu a žurnály nemohou být sdíleny. Správci front s více instancemi v produktu IBM i používají replikaci žurnálu nebo přepínatelné žurnály pro vytváření žurnálů dostupných mezi různými instancemi správce front.

Produkt IBM MQ používá zamykání k zabránění, aby více instancí stejného správce front s více instancemi bylo současně aktivních. Stejné zamykání také zajišťuje, že dva oddělené správce front nemohou nechtěně používat stejnou sadu datových souborů správce front. Pouze jedna instance správce front může mít svůj zámek v daném okamžiku. Z toho vyplývá, že produkt IBM MQ podporuje data správce front uložená v síťovém úložišti, k němuž se přistupuje jako ke sdílenému systému souborů.

Protože ne všechny blokovací protokoly síťových systémů souborů jsou robustní, a protože systém souborů může být nakonfigurován pro výkon spíše než integritu dat, musíte spustit příkaz **amqmfsck** , který otestuje, zda síťový systém souborů bude řídit přístup k datům a žurnály správce front správně. Tento příkaz lze použít 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 114
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.

Linux IBM i 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 pro více instancí v systému Linux nebo Vytvoření správce front pro více instancí 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 za účelem 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 `share`da 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`	

`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.`
	`amqmfsck -a /shared/qmdata`
	
	`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.`	

Tabulka 11. Úspěšné uzamčení na dvou serverech (pokračování)

IBM MQ server 1	IBM MQ server 2
	`> 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...`

`[ 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 za účelem testování integrity zpráv

Chcete-li demonstrovat, že správce front udržuje integritu zpráv během selhání, spusťte ukázkový program IBM MQ MQI client **amqsfhac** paralelně s produktem **amqmfsck** .

Než začnete

Pro tento test jsou zapotřebí čtyři servery. Dva servery pro správce front s více instancemi, jeden pro systém souborů a druhý pro spuštění produktu **amqsfhac** jako aplikace produktu IBM MQ MQI client .

Chcete-li nastavit systém souborů pro správce front s více instancemi, postupujte podle kroků “1” na stránce 115 v části “Ověření chování sdíleného systému souborů na platformě Multiplatforms” na stránce 114 .

Informace o této úloze

Ukázkový program IBM MQ MQI client **amqsfhac** kontroluje, zda správce front používající síťově připojený úložný prostor udržuje integritu dat po selhání. Spusťte **amqsfhac** paralelně s **amqmfsck** , abyste prokázali, že správce front udržuje integritu zpráv během selhání.

Postup

1. Vytvořte správce front s více instancemi na jiném serveru QM1pomocí systému souborů, který jste vytvořili v kroku “1” na stránce 115 v části Procedura.

   Viz téma Vytvoření správce front s více instancemi.
2. Spusťte správce front na obou serverech s vysokou dostupností.

   Na serveru 1:

   ```
   strmqm -x QM1
   ```

   Na serveru 2:

   ```
   strmqm -x QM1
   ```
3. Nastavte připojení klienta ke spuštění produktu **amqsfhac**.

   a) Proceduru použijte v tématu *Ověření instalace produktu IBM MQ* pro platformu nebo platformy, kterou váš podnik používá k nastavení připojení klienta, nebo příklad skriptů v části Opětovně nepřipojitelné ukázky klienta.

   b) Upravte kanál klienta tak, aby měl dvě adresy IP, odpovídající dvěma serverům, které jsou spuštěny na serveru QM1.

   V ukázkovém skriptu upravte:

   ```
   DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
   CONNAME('LOCALHOST(2345)') QMNAME(QM1) REPLACE
   ```

   Do:

   ```
   DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
   CONNAME('server1(2345),server2(2345)') QMNAME(QM1) REPLACE
   ```

   kde server1 a server2 jsou názvy hostitelů těchto dvou serverů a 2345 je port, na kterém naslouchá posluchač kanálu. Obvykle je tato výchozí hodnota nastavena na 1414. Produkt 1414 můžete použít s výchozí konfigurací modulu listener.
4. Vytvořte dvě lokální fronty v produktu QM1 pro test.
   Spusťte následující skript MQSC:

   ```
   DEFINE QLOCAL(TARGETQ) REPLACE
   DEFINE QLOCAL(SIDEQ) REPLACE
   ```
5. Otestujte konfiguraci pomocí produktu **amqsfhac**

   ```
   amqsfhac QM1 TARGETQ SIDEQ 2 2 2
   ```
6. Integrita testovacích zpráv při testování integrity systému souborů.

   Spusťte **amqsfhac** během kroku “5” na stránce 115 z “Ověření chování sdíleného systému souborů na platformě Multiplatforms” na stránce 114.

   ```
   amqsfhac QM1 TARGETQ SIDEQ 10 20 0
   ```

   Pokud zastavíte aktivní instanci správce front, produkt **amqsfhac** se znovu připojí k jiné instanci správce front, jakmile se stane aktivní. Restartujte zastavenou instanci správce front znovu, abyste mohli selhání vrátit při dalším testu. Pravděpodobně bude třeba zvýšit počet iterací na základě experimentů se svým prostředím tak, aby testovací program byl spuštěn dostatečně dlouho, aby došlo k překonání selhání.

Výsledky

Příklad spuštění **amqsfhac** v kroku “6” na stránce 120 je zobrazen 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 testech může produkt MQRC_CALL_INTERRUPTED vykazovat "`Resolving to backed out`". Výsledkem je nerozdílný výsledek. Výsledek závisí na tom, zda byl zápis na disk potvrzen v síťovém úložišti souborů před selháním nebo po jeho výskytu.

Související odkazy

amqmfsck (kontrola systému souborů)

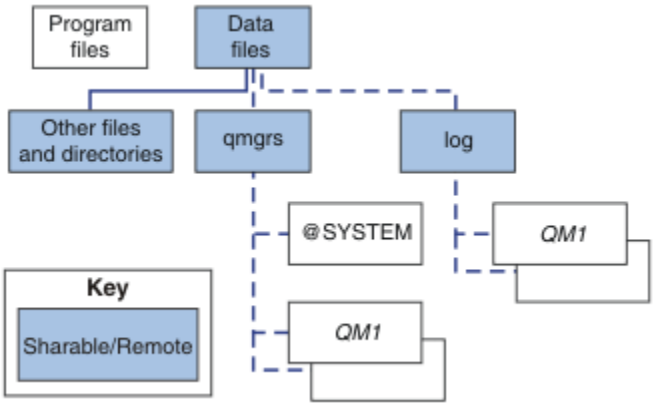
Ukázkové programy s vysokou dostupností

Multi Sdílení souborů IBM MQ na platformách Multiplatforms

Některé soubory produktu IBM MQ jsou přístupné výhradně aktivním správcem front, jiné soubory jsou sdílené.

Soubory IBM MQ jsou rozděleny do programových souborů a datových souborů. Programové soubory jsou obvykle nainstalovány lokálně na každém serveru, na kterém běží IBM MQ. Správci front sdílejí přístup k datovým souborům a adresářům v rámci výchozího datového adresáře. Požadují výhradní přístup ke svým vlastním adresářovým stromům správce front obsaženým v každém z adresářů `qmgrs` a `log` zobrazených v Obrázek 32 na stránce 122.

Obrázek 32 na stránce 122 je vysokoúrovňový pohled na adresářovou strukturu IBM MQ . Zobrazuje adresáře, které lze sdílet mezi správci front a kteří jsou vzdálení. Podrobnosti se liší podle platformy. Tečkovaná čára označuje konfigurovatelné cesty.



Obrázek 32. Celkové zobrazení adresářové struktury 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 v systému Windows. Je sdíleno mezi správci front. Výchozí umístění můžete nastavit jako vzdálenou, ale nesdílet jej mezi různými instalacemi produktu IBM MQ. Atribut `DefaultPrefix` v konfiguraci produktu IBM MQ ukazuje na tuto cestu.

`qmgrs`

Existují dva alternativní způsoby, jak určit umístění dat správce front.

Použití `Předpona`

Atribut `Předpona` určuje umístění adresáře `qmgrs` . Příkaz IBM MQ sestaví název adresáře správce front z názvu správce front a vytvoří jej jako podadresář adresáře `qmgrs` .

Atribut `Předpona` je umístěn ve stanze QueueManager a je zděděn od hodnoty v atributu `DefaultPrefix` . Ve výchozím nastavení správce front pro administrativní zjednodušení obvykle sdílí stejný adresář `qmgrs` .

Objekt stanza `QueueManager` je umístěn v souboru `mqs.ini` .

Změníte-li umístění adresáře `qmgrs` pro žádného správce front, je třeba změnit hodnotu atributu `Předpona` .

Atribut `Předpona` pro adresář `QM1` v produktu Obrázek 32 na stránce 122 pro platformu AIX and Linux je následující:

```
Prefix=/var/mqm
```

Použití `DataPath`

Atribut `DataPath` určuje umístění datového adresáře správce front.

Atribut `DataPath` uvádí úplnou cestu, včetně názvu datového adresáře správce front. Atribut `DataPath` se liší od atributu `Předpona` , který určuje neúplnou cestu k datovému adresáři správce front.

Atribut `DataPath` , je-li zadán, je umístěn ve stanze QueueManager . Pokud byla zadána, má přednost před každou hodnotou atributu `Předpona` .

Objekt stanza `QueueManager` je umístěn v souboru `mqs.ini` .

Změníte-li umístění datového adresáře správce front pro libovolného správce front, musíte změnit hodnotu atributu `DataPath` .

Atribut DataPath pro adresář QM1 v produktu Obrázek 32 na stránce 122 pro platformu AIX nebo Linux je:

```
DataPath=/var/mqm/qmgrs/QM1
```

log

Adresář protokolů je určen samostatně pro každého správce front v sekci Log v konfiguraci správce front. Konfigurace správce front je v produktu qm.ini.

Podadresáře *DataPath*/*QmgrName*/@IPCC

Podadresáře *DataPath*/*QmgrName*/@IPCC se nacházejí v cestě ke sdílenému adresáři. Používají se k vytvoření cesty k adresáři pro objekty systému souborů IPC. Je třeba rozlišovat obor názvů správce front, když je správce front sdílen mezi systémy.

Systémové objekty systému souborů IPC musí být odlišeny systémem. Do cesty k adresáři se přidá podadresář pro každý systém, v němž je spuštěn správce front, je uveden v tématu Obrázek 33 na stránce 123.

```
DataPath/QmgrName/@IPCC/esem/myHostName/
```

Obrázek 33. Příklad podadresáře IPC

myHostName je až prvních 20 znaků z názvu hostitele vráceného operačním systémem. Na některých systémech může být název hostitele až 64 znaků dlouhý před oseknutím. Vygenerovaná hodnota *myHostName* může způsobit problém ze dvou důvodů:

1. Prvních 20 znaků není jedinečné.
2. Název hostitele je generován algoritmem DHCP, který nealokuje vždy stejný název hostitele do systému.

V těchto případech nastavte *myHostName* pomocí proměnné prostředí MQS_IPC_HOST ; viz Obrázek 34 na stránce 123.

```
export MQS_IPC_HOST= myHostName
```

Obrázek 34. Příklad: nastavení MQS_IPC_HOST

Ostatní soubory a adresáře

Jiné soubory a adresáře, jako je adresář obsahující trasovací soubory a společný protokol chyb, jsou obvykle sdíleny a uchovány v lokálním systému souborů.

S podporou sdílených systémů souborů IBM MQ spravuje výhradní přístup k těmto souborům pomocí zámků systému souborů. Zámek systému souborů umožňuje aktivní v daném okamžiku pouze jednu instanci určitého správce front.

Když spustíte první instanci konkrétního správce front, převezme vlastnictví svého adresáře správce front. Pokud spustíte druhou instanci, může převzít vlastnictví pouze v případě, že se první instance zastavila. Je-li první správce front stále spuštěn, druhá instance se nespustí a ohlásí, že správce front je spuštěn jinde. Pokud byl zastaven první správce front, převezme vlastnictví správce front i druhý správce front a stane se spuštěným správcem front.

Můžete zautomatizovat proceduru druhého správce front, který přebírá řízení od prvního. Spusťte prvního správce front s volbou strmqm -x , která povoluje jinému správci front převzít jeho obsah. Druhý správce front pak před pokusem o převzetí vlastnictví souborů správce front vyčká, dokud se soubory správce front nezamkne, a spustí se.

Linux AIX Adresářová struktura v systémech AIX and Linux

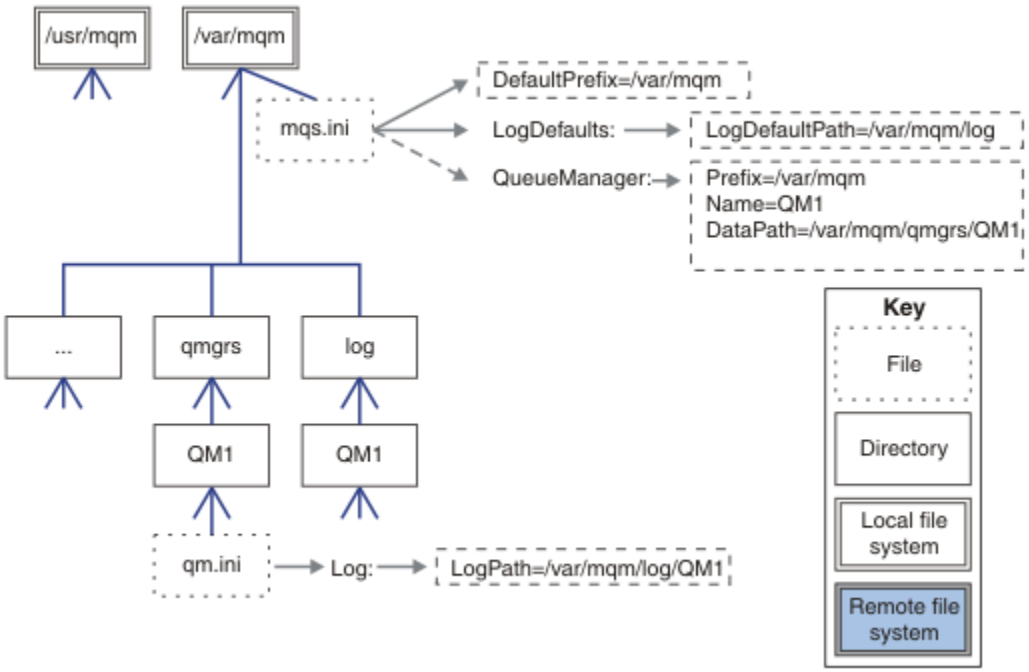
Adresářová struktura produktu IBM MQ v systémech AIX and Linux může být mapována na různé systémy souborů pro snadnější správu, lepší výkon a vyšší spolehlivost.

Využijte flexibilní strukturu adresářů produktu IBM MQ k využití výhod sdílených souborových systémů pro spouštění správců front s více instancemi.

Pomocí příkazu **crtmqm** *QM1* vytvořte adresářovou strukturu zobrazenou 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 atributu .ini jsou kvůli přehlednosti vynechány a mangování může být změněno jiným názvem správce front. Názvy systémů souborů se liší v různých systémech.

V typické instalaci se každý správce front, kterého vytvoříte, odkazuje na obecné adresáře `log` a `qmgrs` v lokálním systému souborů. V konfiguraci s více instancemi jsou adresáře `log` a `qmgrs` umístěny v síťovém systému souborů sdíleném s jinou instalací produktu IBM MQ.

Obrázek 35 na stránce 124 zobrazuje výchozí konfiguraci pro IBM MQ v7.R v systému AIX , kde R je vydání produktu. Příklady alternativních konfigurací s více instancemi najdete v tématu“Příklad konfigurací adresáře na systémech AIX and Linux” na stránce 129.



Obrázek 35. Příklad výchozí struktury adresářů IBM MQ pro systémy AIX and Linux

Produkt je při výchozím nastavení nainstalován do produktu `/usr/mqm` na systémech AIX a `/opt/mqm` na jiných systémech. Pracovní adresáře jsou nainstalovány do adresáře `/var/mqm` .

Poznámka: Pokud jste vytvořili systém souborů `/var/mqm` před instalací produktu IBM MQ , ujistěte se, že má uživatel mqm oprávnění k úplnému adresáři, jako je například režim souboru 755.

Poznámka: Adresář `/var/mqm/errors` by měl být samostatným systémem souborů, aby se zabránilo tomu, že FFDCs vytvoří správce front v zaplnění systému souborů, který obsahuje `/var/mqm`.

Další informace naleznete v tématu Vytvoření systémů souborů v systémech AIX and Linux .

Adresáře `log` a `qmgrs` se zobrazí ve svých výchozích umístěních, jak je definuje výchozí hodnoty atributů `LogDefaultPath` a `DefaultPrefix` v souboru `mqs.ini` . Je-li vytvořen správce front, je při výchozím nastavení vytvořen datový adresář správce front v produktu *`DefaultPrefix`*`/qmgrs`a v adresáři *`LogDefaultPath`*`/log`se nachází adresář souborů protokolu. `LogDefaultPath` a `DefaultPrefix` mají vliv pouze tehdy, jsou-li správci front a soubory protokolu vytvářeny při výchozím nastavení. Skutečné

umístění adresáře správce front je uloženo v souboru `mqs.ini` a umístění adresáře souboru protokolu se uloží do souboru `qm.ini` .

Adresář souboru protokolu pro správce front je definován v souboru `qm.ini` v atributu `LogPath` . Použijte volbu `-ld` v příkazu **crtmqm** k nastavení atributu `LogPath` pro správce front, například **crtmqm** `-ld` *LogPath* `QM1` . Vynecháte-li parametr `ld` , použije se místo toho hodnota `LogDefaultPath` .

Datový adresář správce front je definován v atributu `DataPath` ve stanze `QueueManager` v souboru `mqs.ini` . Volbu `-md` příkazu **crtmqm** použijte k nastavení parametru `DataPath` pro správce front, například **crtmqm** `-md` *DataPath* `QM1` . Pokud vynecháte parametr `md` , bude místo toho použita hodnota atributu `DefaultPrefix` nebo `Předpona` . `Předpona` má přednost před `DefaultPrefix`.

Zpravidla vytvořte `QM1` specifikující jak protokol protokolů, tak datové adresáře v jednom příkazu.

```
 crtmqm
-md DataPath -ld
LogPath QM1
```

Můžete upravit umístění protokolu správce front a datových adresářů existujícího správce front úpravou atributů `DataPath` a `LogPath` v souboru `qm.ini` , když je správce front zastaven.

Cesta k adresáři `errors` , stejně jako cesty ke všem ostatním adresářům v produktu `/var/mqm`, není modifikovatelná. Avšak adresáře mohou být připojeny na různých systémech souborů nebo symbolicky propojeny s různými adresáři.

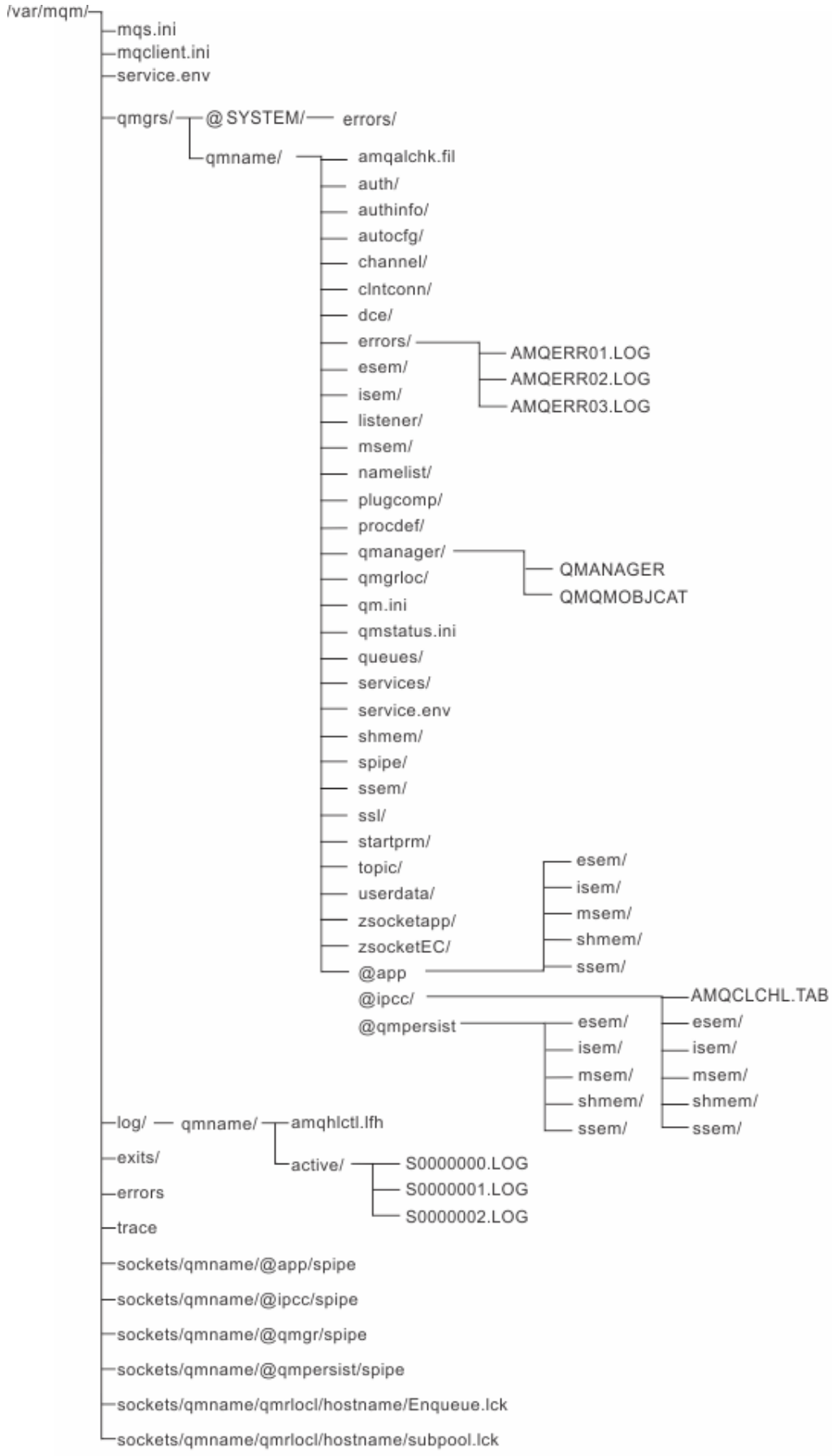
Linux AIX *Obsah adresáře v systémech AIX and Linux*

Obsah adresářů přidružených ke správci front.

Informace o umístění souborů produktu naleznete v tématu Výběr umístění instalace .

Další informace o konfiguraci alternativních adresářů najdete v tématu “Plánování podpory systému souborů na více platformách” na stránce 111.

V 9.2.0 Následující adresářová struktura je zástupkyně produktu IBM MQ poté, co byl správce front používán již nějakou dobu. Skutečná struktura, která závisí na tom, které operace ve správci front nastaly, se liší.


/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, nikoli na jednotlivé správce front.

Tabulka 13. Dokumentovaný obsah adresáře /var/mqm v systému AIX and Linux	
Název adresáře nebo souboru	**Obsah**
mqs.ini	Konfigurační soubor pro celou instalaci produktu IBM MQ , který je načten při spuštění správce front. Cesta k souboru modifikovatelná pomocí proměnné prostředí **AMQ_MQS_INI_LOCATION** . Ujistěte se, že je nastavena a exportována v shellu, ve kterém je spuštěn příkaz **strmqm** .
mqclient.ini	Výchozí konfigurační soubor klienta načtený programy IBM MQ MQI client . Cesta k souboru modifikovatelná pomocí proměnné prostředí **MQCLNTCF** .
service.env	Obsahuje proměnné prostředí rozsahu stroje pro proces služby. Cesta k souboru byla opravena.
chyby/	Protokoly chyb rozsahu stroje a soubory FFST . Cesta k adresáři byla opravena. Viz také FFST: systémy IBM MQ for UNIX a Linux.
sokety/	Obsahuje informace o každém správci front pouze pro účely systému.
trasovat/	Trasovací soubory. Cesta k adresáři byla opravena.
web/	Adresář serveru mqweb.
ukončení/	Výchozí adresář obsahující uživatelské programy kanálu uživatele. Umístění lze upravit ve stanzách ApiExit v souboru mqs.ini .
exits64/	

/var/mqm/qmgrs/*qmname*/

/var/mqm/qmgrs/*qmname*/ obsahuje adresáře a soubory pro správce front. Tento adresář je uzamknut pro výhradní přístup k aktivní instanci správce front. Cesta k adresáři je přímo modifikovatelná v souboru mqs.ini , nebo pomocí volby **md** příkazu **crtmqm** .

Tabulka 14. Dokumentovaný obsah adresáře /var/mqm/qmgrs/qmname v systému AIX and Linux	
Název adresáře nebo souboru	**Obsah**
qm.ini	Konfigurační soubor správce front, načten při spuštění správce front.
chyby/	Protokoly chyb rozsahu správce front. Hodnota *qmname* = @system obsahuje zprávy související s kanálem pro neznámého nebo nedostupného správce front.

Tabulka 14. Dokumentovaný obsah adresáře /var/mqm/qmgrs/qmname v systému AIX and Linux (pokračování)	
Název adresáře nebo souboru	**Obsah**
@ipcc/ AMQCLCHL.TAB	Výchozí řídicí tabulka kanálů klienta, vytvořená serverem IBM MQ a čte programy IBM MQ MQI client . Cesta k souboru modifikovatelná pomocí proměnných prostředí **MQCHLLIB** a **MQCHLTAB** .
QMANAGER	Soubor objektů správce front: QMANAGER Katalog objektů správce front: QMQMOBJCAT
authinfo/	Každý objekt definovaný v rámci správce front je přidružen k souboru v těchto adresářích. Název souboru se přibližně shoduje s názvem definice; viz téma Základní informace o názvech souborů produktu IBM MQ.
kanál/	
clntconn/	
modul listener/	
seznam názvů/	
procdef/	
fronty/	
služby/	
témata/	
...	Ostatní adresáře používané produktem IBM MQ, jako např. @ipcc, lze upravit pouze pomocí produktu IBM MQ.
V 9.2.0 **uživatelská data/**	Lze použít k ukládání trvalého stavu aplikací (může být produktem RDQM použit při přesunu správců front do různých uzlů-viz téma Uložení stavu trvalé aplikace.)
V 9.2.0 ***DataPath*\autocfg**	Používá se pro automatickou konfiguraci

/var/mqm/log/*qmname*/

/var/mqm/log/*qmname*/ obsahuje soubory protokolu správce front. Tento adresář je uzamknut pro výhradní přístup k aktivní instanci správce front. Cesta k adresáři je modifikovatelná v souboru qm.ini , nebo pomocí volby **ld** příkazu **crtmqm** .

Tabulka 15. Dokumentovaný obsah adresáře /var/mqm/log/qmname v systému AIX and Linux	
Název adresáře nebo souboru	**Obsah**
amqhlctl.lfh	Řídicí soubor protokolu.
aktivní/	Tento adresář obsahuje soubory s protokolem s číslem S0000000.LOG, S0000001.LOG, S0000002.LOGatd.

/opt/mqm

/opt/mqm je standardně instalační adresář na většině platforem. Další informace o množství prostoru, který potřebujete pro instalační adresář na platformě nebo na platformách, které používá váš podnik, naleznete v příručce “Požadavky na prostor na disku na platformách” na stránce 108 .

Linux AIX *Příklad konfigurací adresáře na systémech AIX and Linux*

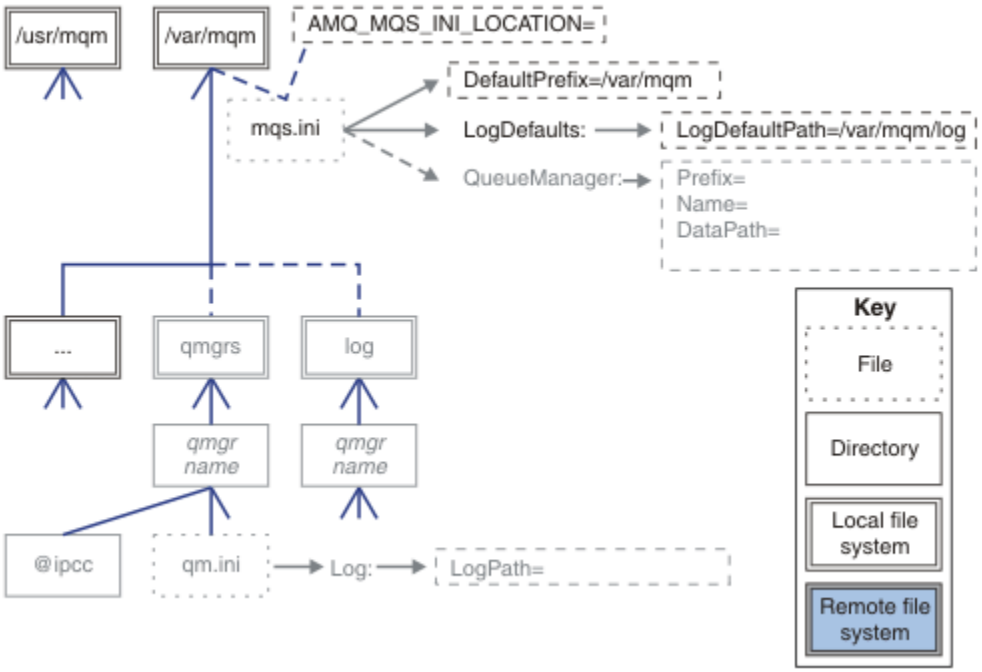
Příklady konfigurace alternativních systémů souborů v systémech AIX and Linux .

Adresářovou strukturu produktu IBM MQ můžete přizpůsobit různým způsobem, abyste dosáhli řady různých cílů.

- Chcete-li konfigurovat správce front pro více instancí, umístěte adresáře qmgrs a log na vzdálené sdílené systémy souborů.
- Použijte oddělené systémy souborů pro adresáře dat a protokolů a přidělte adresáře na různé disky, abyste zlepšili výkon tím, že snížíte soupeření vstupu/výstupu.
- Použijte rychlejší úložná zařízení pro adresáře, které mají větší vliv na výkon. Latence fyzického zařízení je často důležitějším faktorem při výkonu trvalého systému zpráv, než je to, zda je zařízení připojeno lokálně nebo vzdáleně. Následující seznam ukazuje, které adresáře jsou nejvíce a nejméně citlivé na výkon.
  1. log
  2. qmgrs
  3. Ostatní adresáře, včetně /usr/mqm
- Vytvořte adresáře qmgrs a log v systémech souborů, které jsou alokovány pro úložiště s dobrou odolností, jako je například redundantní diskové pole.
- Je lepší ukládat běžné protokoly chyb do var/mqm/errors, lokálně, spíše než na síťový systém souborů, takže chyba související se síťovým systémem souborů může být protokolována.

Obrázek 36 na stránce 130 je šablona, ze které jsou odvozeny alternativní struktury adresáře IBM MQ . Tečkované čáry v šabloně představují cesty, které lze konfigurovat. V uvedených příkladech jsou tečkované čáry nahrazeny pevnými řádky, které odpovídají informacím o konfiguraci uloženým v proměnné prostředí AMQ_MQS_INI_LOCATION a v souborech mqs.ini a qm.ini .

Poznámka: Informace o cestě se zobrazí tak, jak se objevují v souborech mqs.ini nebo qm.ini . Zadáte-li v příkazu **crtmqm** parametry cesty, vynechte název adresáře správce front: název správce front bude přidán do cesty produktem IBM MQ.



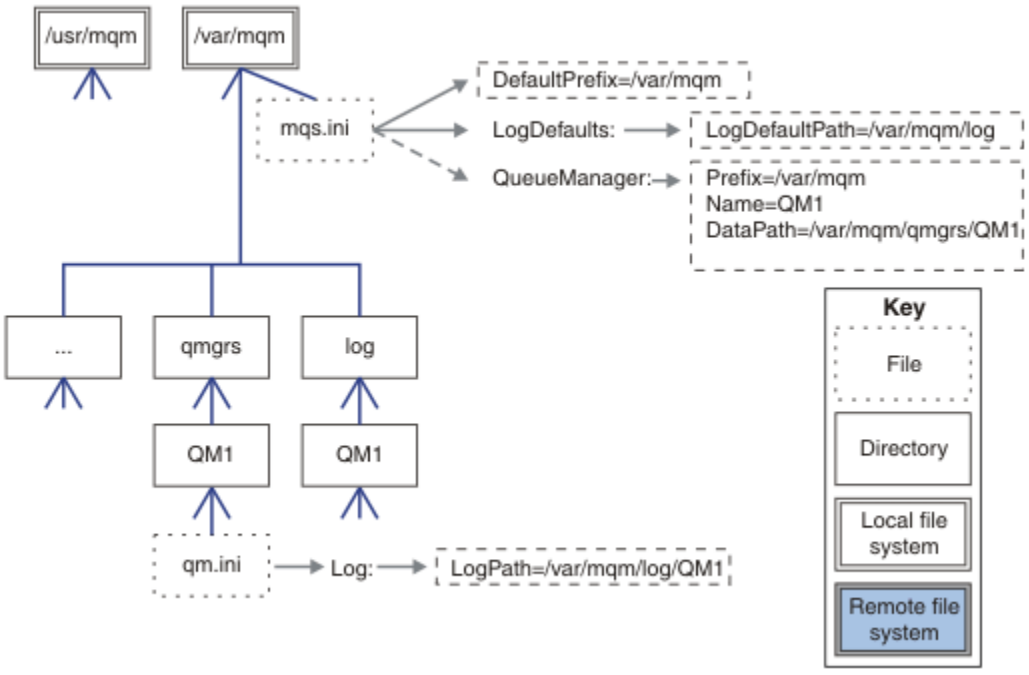
Obrázek 36. Šablona vzoru struktury adresáře

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 oddíl pro správce front QM1 vytvořený odkazem na hodnotu `DefaultPrefix`. Objekt stanza `Log` v souboru `qm.ini` má hodnotu pro `LogPath`, který je nastaven odkazem na `LogDefaultPath` v `mqs.ini`.

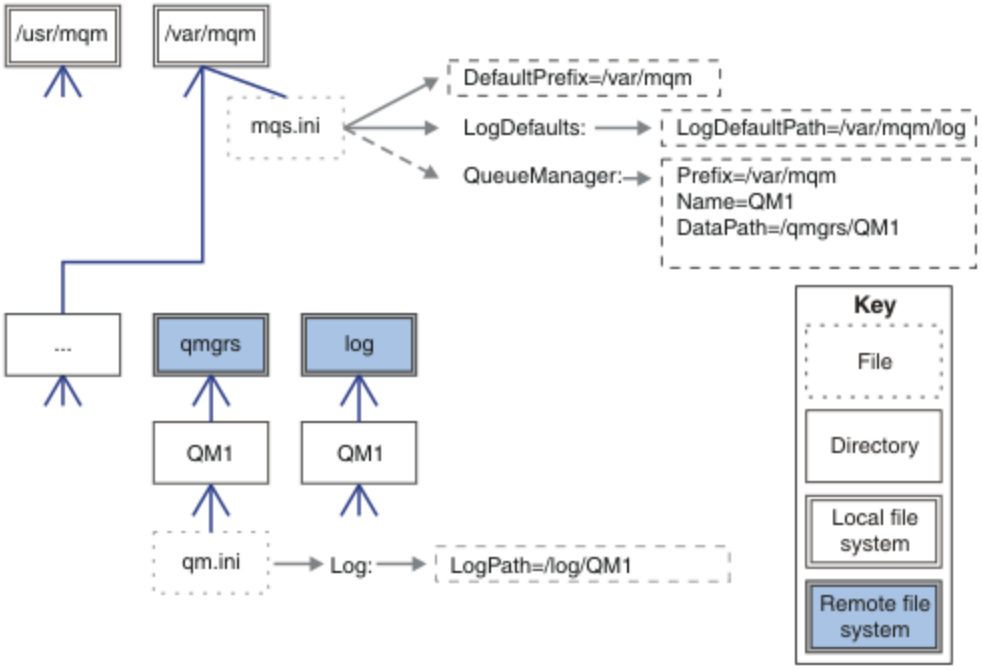
Chcete-li přepsat výchozí hodnoty `DataPath` a `LogPath`, použijte volitelné parametry **crtmqm** .



Obrázek 37. Příklad výchozí struktury adresářů IBM MQ pro systémy AIX and Linux

Sdílet výchozí adresáře qmgrs a log)

Alternativou k “Sdílet vše” na stránce 132je sdílení adresářů qmgrs a log odděleně (Obrázek 38 na stránce 131). V této konfiguraci není třeba nastavit AMQ_MQS_INI_LOCATION jako výchozí soubor mqs.ini , který je uložen v lokálním systému souborů /var/mqm . Soubory a adresáře, jako například mqclient.ini a mqserver.ini , nejsou také sdíleny.

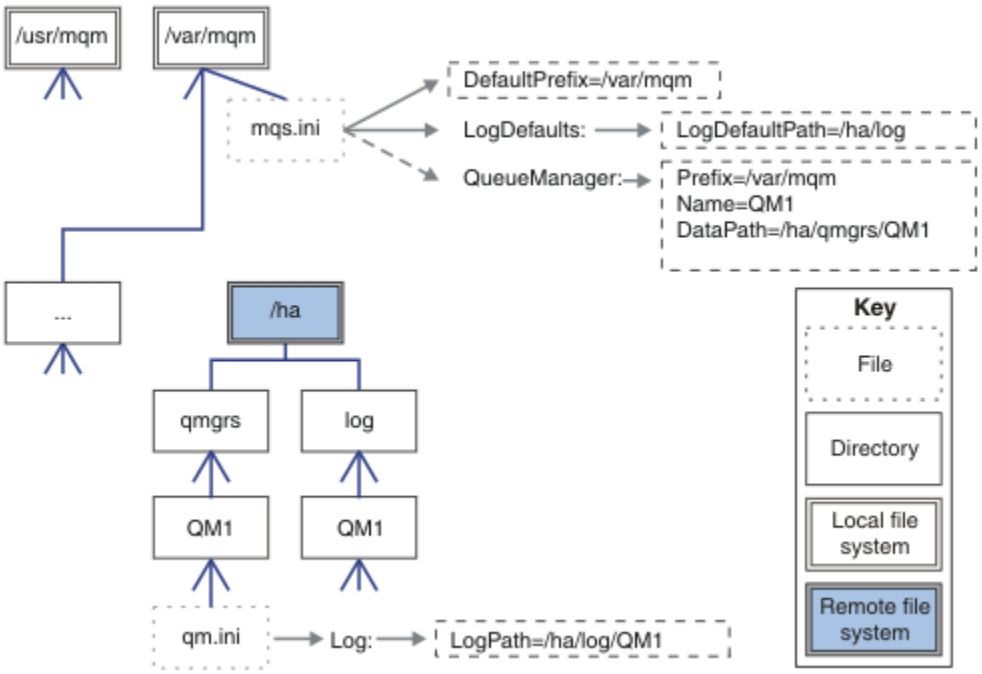


Obrázek 38. Sdílení adresářů qmgrs a log

Sdílení pojmenovaných adresářů qmgrs a log

Konfigurace v produktu Obrázek 39 na stránce 132 umístí log a qmgrs do obecného jmenovaného vzdáleného sdíleného systému souborů nazvaného /ha. Stejnou fyzickou konfiguraci lze vytvořit dvěma různými způsoby.

1. Nastavte LogDefaultPath=/ha a pak spusťte příkaz **crtmqm** - md */haqmgrs* QM1. Výsledek je přesně tak, jak je ilustrováno v Obrázek 39 na stránce 132.
2. Ponechejte výchozí cesty nezměněny a pak spusťte příkaz, **crtmqm** - ld */ha/log* - md */haqmgrs* QM1.



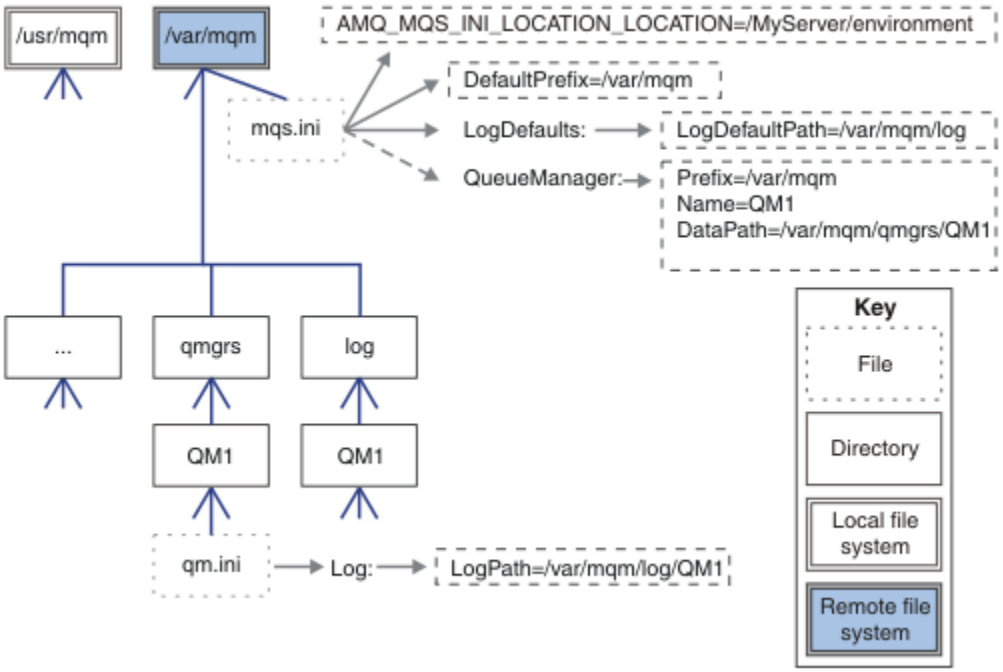
Obrázek 39. Sdílení pojmenovaných adresářů `qmgrs` a `log`

Sdílet vše

Obrázek 40 na stránce 133 je jednoduchá konfigurace pro systém s rychlým síťovým úložištěm souborů.

Připojte `/var/mqm` jako vzdálený sdílený systém souborů. Standardně, když spustíte QM1, vyhledá `/var/mqm`, najde ho na sdíleném systému souborů a přečte soubor `mqs.ini` v `/var/mqm`. Místo použití jednoho souboru `/var/mqm/mqs.ini` pro správce front na všech serverech můžete nastavit proměnnou prostředí `AMQ_MQS_INI_LOCATION` na každém serveru tak, aby ukazovala na různé soubory `mqs.ini` .

Poznámka: Obsah generického souboru chyb v produktu `/var/mqm/errors/` je sdílen mezi správci front na různých serverech.



Obrázek 40. Sdílet vše

Všimněte si, že toto nemůžete použít pro správce front s více instancemi. Důvodem je to, že je nezbytné, aby každý hostitel ve správci front s více instancemi měl vlastní lokální kopii produktu `/var/mqm` ke sledování lokálních dat, jako jsou například semafory a sdílená paměť. Tyto entity nemohou být sdíleny mezi hostiteli.

Windows Adresářová struktura v systémech Windows

Postup vyhledání informací o konfiguraci správce front a adresářů 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.

Pokud chcete 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** .

Spuštěním 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 nakonfigurovat správce front s více instancemi, musí být datové adresáře protokolu a dat umístěny v síťovém úložišti, pokud možno na jiném serveru, na některý ze serverů, na kterých jsou spuštěny instance správce front.

V příkazu **crtmqm** , **-md** a **-ld**jsou k dispozici dva parametry, aby bylo snazší zadat umístění dat správce front a adresářů protokolů. Efekt zadání parametru **-md** je čtyřnásobně:

1. Stanza `mqs.ini` `QueueManager\`*`QmgrName`* obsahuje novou proměnnou, *DataPath*, která ukazuje na datový adresář správce front. Na rozdíl od proměnné *Předpona* cesta obsahuje název adresáře správce front.
2. Informace o konfiguraci správce front uložené v souboru mqs.ini jsou zmenšena na hodnoty *Název*, *Předpona*, *Adresář* a *DataPath*.

Windows *Obsah adresářů*

Vypíše umístění a obsah adresářů IBM MQ .

Konfigurace produktu IBM MQ má tři hlavní sady souborů a adresářů:

1. Spustitelný soubor a ostatní soubory jen pro čtení, které jsou aktualizovány pouze při použití údržby. Příklad:
   - Soubor Readme
   - Modul plug-in a soubory nápovědy modulu plug-in produktu IBM MQ Explorer
   - Soubory s licencemi

   Tyto soubory jsou popsány v tématu Tabulka 16 na stránce 134.
2. Potenciálně upravitelné soubory a adresáře, které nejsou specifické pro konkrétního správce front. Tyto soubory a adresáře jsou popsány v tématu Tabulka 17 na stránce 135.
3. Soubory a adresáře, které jsou specifické pro každého správce front na serveru. Tyto soubory a adresáře jsou popsány v tématu Tabulka 18 na stránce 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 produktu IBM MQ specifickou 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 (64bitové)
FilePath\conv	Tabulky pro převod dat
FilePath\doc	Soubory nápovědy průvodce
FilePath\MQExplorer	Moduly plug-in pro průzkumníka a průzkumníka Eclipse
FilePath\gskit8	Globální sada zabezpečení
FilePath\java	Prostředky produktu Java , včetně prostředí JRE
FilePath\licenses	Informace o licenci
FilePath\Non_IBM_License	Informace o licenci

Tabulka 16. Adresáře a soubory v adresáři `FilePath` (pokračování)	
Cesta k souboru	**Obsah**
`FilePath``\properties`	Používá se interně
`FilePath``\Tivoli`	
`FilePath``\tools`	Vývojové zdroje a ukázky
`FilePath``\web`	Popsáno v souboru IBM MQ Console and REST API installation component file structure for non-editovatelné soubory.
`FilePath``\Uninst`	Používá se interně
`FilePath``\README.TXT`	Soubor Readme

Adresáře, které nejsou specifické pro správce front

Některé adresáře obsahují soubory, jako jsou trasovací soubory a protokoly chyb, které nejsou specifické pro konkrétního správce front. Proměnná *DefaultPrefix* obsahuje cestu k těmto adresářům. Položka *DefaultPrefix* je součástí stanzy `AllQueueManagers` .

Tabulka 17. Adresáře a soubory v adresáři `DefaultPrefix`	
Cesta k souboru	**Obsah**
`DefaultPrefix``\config`	Používá se interně
`DefaultPrefix``\conv`	Řídicí soubor pro převod `ccsid_part2.tbl` a `ccsid.tbl` `data` je popsán v tématu Převod dat
`DefaultPrefix``\errors`	Protokoly chyb nesprávců front, `AMQERR` *`nn`*`.LOG`
`DefaultPrefix``\exits`	Ukončovací programy kanálu
`DefaultPrefix``\exits64`	Ukončovací programy kanálu (64 bitů)
`DefaultPrefix``\ipc`	Nepoužito
`DefaultPrefix``\qmgrs`	Popsáno v Tabulka 18 na stránce 135
`DefaultPrefix``\trace`	Trasovací soubory
`DefaultPrefix``\web`	Popsáno v souboru IBM MQ Console a struktura souboru komponent instalační komponenty produktu REST API pro soubory upravitelné uživatelem
`DefaultPrefix``\amqmjpse.txt`	Používá se interně

Adresáře správce front

Při vytváření správce front je vytvořena nová sada adresářů, která je specifická pro správce front.

Pokud vytvoříte správce front s argumentem **`-md`** *`filepath`* , cesta se uloží do proměnné *DataPath* ve stanze správce front v souboru mqs.ini . Pokud vytvoříte správce front bez nastavení parametru **`-md`** *`filepath`* , vytvoří se adresáře správce front v cestě uložené v souboru *DefaultPrefix*a cesta je zkopírována do proměnné *Předpona* ve stanze správce front v souboru mqs.ini .

Tabulka 18. Adresáře a soubory v adresářích `DataPath` a `Prefix``\qmgrs\`*`QmgrName`*	
Cesta k souboru	**Obsah**
`DataPath``\@ipcc`	Výchozí umístění pro `AMQCLCHL.TAB`, tabulka připojení klienta.

Tabulka 18. Adresáře a soubory v adresářích DataPath a Prefix\qmgrs\QmgrName (pokračování)	
Cesta k souboru	**Obsah**
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
V 9.2.0 *DataPath*\userdata	Lze použít k ukládání trvalého stavu aplikací.
Prefix\qmgrs*QmgrName*	Používá se interně
Prefix\qmgrs\@SYSTEM	Nepoužito
Prefix\qmgrs\@SYSTEM\errors	
V 9.2.0 *DataPath*\autocfg	Používá se pro automatickou konfiguraci

IBM i Adresářová struktura v systému IBM i

Je dán popis IFS a adresářová struktura IBM MQ IFS je popsána pro server, klienta a Java.

Integrovaný systém souborů (IFS) je část IBM i , která podporuje vstupní/výstupní tok a správu paměti podobně jako osobní počítač, AIX and Linux operační systémy a zároveň poskytuje integrující strukturu pro všechny informace uložené na serveru.

Názvy adresářů IBM i začínají znakem & (ampersand) místo znaku @ (at). Například @system na IBM i je &system.

Kořenový systém souborů IFS pro server IBM MQ

Když instalujete produkt IBM MQ Server for IBM i, vytvoří se následující adresáře v kořenovém systému souborů IFS.

ProdData:

Přehled

```
QIBM
   '-- ProdData
      '-- mqm
      '-- doc
      '-- inc
      '-- lib
      '-- samp
      '-- licenses
      '-- LicenseDoc
      '-- 5724H72_V8R0M0
```

/QIBM/ProdData/mqm
Níže uvedené podadresáře obsahují všechna data produktu, například třídy C + +, soubory s formátem trasování a soubory s licencemi. Data v tomto adresáři se odstraní a nahradí se pokaždé, když je produkt nainstalován.

/QIBM/ProdData/mqm/doc
Popis příkazů pro příkazy CL se poskytuje ve formátu HTML a je instalován zde.

/QIBM/ProdData/mqm/inc
Soubory záhlaví pro kompilaci vašich programů v jazyce C nebo C + +.

/QIBM/ProdData/mqm/lib
Pomocné soubory používané produktem MQ.

/QIBM/ProdData/mqm/samp
Další vzorky.

/QIBM/ProdData/mqm/licenses.
Soubory s licencemi. Tyto dva soubory pro každý jazyk jsou pojmenovány jako LA_ *xx* a LI_ *xx* , kde *xx* je dvouznakový identifikátor jazyka pro každý zadaný jazyk.

Soubory licenčních smluv se ukládají také do následujícího adresáře:

/QIBM/ProdData/LicenseDoc/5724H72_V8R0M0
Soubory s licencemi. Soubory jsou pojmenovány jako 5724H72_V8R0M0_ *xx* , kde *xx* je 2 nebo 5 znaků identifikátoru jazyka pro každý zadaný jazyk.

UserData:

Přehled

```
QIBM
   '-- UserData
      '-- mqm
      '-- errors
      '-- trace
      '-- qmgrs
      '-- &system
      '-- qmgrname1
      '-- qmgrname2
      '-- and so on
```

/QIBM/UserData/mqm
Níže uvedené podadresáře obsahují všechna uživatelská data vztahující se ke správcům front.

Když instalujete produkt, vytvoří se soubor mqs.ini v adresáři /QIBM/UserData/mqm/ (pokud již neexistuje z předchozí instalace).

Při vytváření správce front je soubor qm.ini vytvořen v adresáři /QIBM/UserData/mqm/qmgrs/*QMGRNAME* /(kde *QMGRNAME* je název správce front).

Data v adresářích se uchovají, když je produkt odstraněn.

Kořenový systém souborů IFS pro IBM MQ MQI client

Když instalujete produkt IBM MQ MQI client for IBM i, následující adresáře vytvořené v kořenovém systému souborů IFS:

ProdData:

Přehled

```
QIBM
   '-- ProdData
      '-- mqm
      '-- lib
```

/QIBM/ProdData/mqm
Podadresáře pod tímto adresářem obsahují všechna data produktu. Data v tomto adresáři se odstraní a nahradí se 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

Když instalujete produkt IBM MQ Java v systému IBM i, jsou v kořenovém systému souborů IFS vytvořeny následující adresáře:

ProdData:

Přehled

```
QIBM
   '-- ProdData
      '-- mqm
      '-- java
      '--samples
      '-- bin
      '-- lib
```

/QIBM/ProdData/mqm/java
Níže uvedené podadresáře obsahují všechna data produktu, včetně tříd produktu Java . Data v tomto adresáři se odstraní a nahradí se pokaždé, když je produkt nahrazen.

/QIBM/ProdData/mqm/java/samples
Níže uvedené podadresáře obsahují všechny ukázky tříd a dat produktu Java .

Knihovny vytvořené instalací serveru a klienta

Instalace serveru nebo klienta produktu IBM MQ vytvoří následující knihovny:

- QMQM

  Knihovna produktu.

- QMQMSAMP

  Knihovna ukázek (pokud se rozhodnete instalovat ukázky).

- QMxxxx

  Pouze server.

  Při každém vytvoření správce front produkt IBM MQ automaticky vytvoří přidruženou knihovnu s názvem, například QMxxxx , kde je xxxx odvozen od názvu správce front. Tato knihovna obsahuje objekty, které jsou specifické pro správce front, včetně žurnálů a přidružených zásobníků. Při výchozím nastavení je název této knihovny odvozen z názvu správce front s předponou QM. Například u správce front s názvem TEST bude knihovna nazývána QMTEST.

  Poznámka: Při vytváření správce front můžete zadat název jeho knihovny, pokud chcete. Příklad:

  ```
  CRTMQM MQMNAME(TEST) MQMLIB(TESTLIB)
  ```

  Můžete použít příkaz WRKLIB, abyste vypsali všechny knihovny, které IBM MQ pro IBM i vytvořil. V případě knihoven správce front se zobrazí text QMGR: QMGRNAME. Formát příkazu je:

  ```
  WRKLIB LIB(QM*)
  ```

  Tyto knihovny přidružené ke správci front se zachovají, když je produkt odstraněn.

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 metodu Java **`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 Výběr kruhového nebo lineárního protokolování na více platformách

V produktu IBM MQmůžete zvolit kruhové nebo lineární protokolování. Následující informace vám poskytují přehled obou typů.

Výhody kruhové protokolování

Hlavní výhody kruhového protokolování jsou, že kruhové protokolování je:

- Snazší spravovat.

  Jakmile jste nakonfigurovali kruhové protokolování správně pro pracovní zátěž, není třeba žádná další administrace. vzhledem k tomu, že pro lineární protokolování je třeba zaznamenávat obrazy médií a protokolovat oblasti, které již nejsou zapotřebí, aby byly archivovány nebo odstraňovány.

- Lepší výkon

  Cyklické protokolování má lepší než lineární protokolování, protože kruhové protokolování je schopné znovu použít oblasti protokolu, které již byly formátovány. Vzhledem k tomu, že lineární protokolování musí přidělit nové oblasti pro rozšíření protokolu a formátovat je.

Další informace viz Správa protokolů .

Výhody lineárního protokolování

Hlavní výhodou lineárního protokolování je to, že lineární protokolování poskytuje ochranu proti dalším selháním.

Ani kruhové, ani lineární protokolování se chrání proti poškozenému nebo odstraněnému protokolu, zprávám nebo frontám, které byly odstraněny aplikacemi nebo administrátorem.

Lineární protokolování (ale ne kruhové) umožňuje obnovu poškozených objektů. Takže lineární protokolování poskytuje ochranu před porušenými nebo odstraněnými soubory ve frontě, protože tyto poškozené fronty lze obnovit z lineárního protokolu.

Cirkulární a lineární ochrana proti výpadku proudu a selhání komunikace, jak je popsáno v tématu Zotavení po výpadku proudu nebo selhání komunikace.

Další aspekty

To, zda zvolíte lineární nebo kruhové, závisí na tom, kolik redundance potřebujete.

Existuje nákladovost výběru vyšší redundance, která je lineární protokolování, způsobená nákladními náklady a náklady na administraci.

Další informace naleznete v tématu Typy protokolování .

AIX Sdílená paměť v systému AIX

Pokud se určité typy aplikací nepodaří připojit z důvodu omezení paměti AIX , lze ve většině případů toto řešení vyřešit nastavením proměnné prostředí EXTSHM=ON.

Některé 32bitové procesy v systému AIX mohou narazit na omezení operačního systému, které má vliv na jejich schopnost připojit se ke správcům front produktu IBM MQ . Každé standardní připojení k produktu IBM MQ používá sdílenou paměť, ale na rozdíl od jiných platforem produktu UNIX umožňuje produkt AIX 32bitovým procesům připojit pouze 11 sdílené sady paměti.

Většina 32bitových procesů se tento limit nezobrazí, ale aplikace s vysokými požadavky na paměť se mohou nepřipojit k produktu IBM MQ s kódem příčiny 2102: MQRC_RESOURCE_PROBLÉM. Tuto chybu mohou zobrazit následující typy aplikací:

- Programy spuštěné v 32bitovém virtuálním počítači Java
- Programy používající velké nebo velmi velké modely paměti
- Programy, které se připojují k mnoha správcům front nebo databázím
- Programy, které se připojují ke sdíleným paměťovým sadám, na jejich vlastní

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 brání této chybě ve většině případů, ale je nekompatibilní s programy, které používají volbu SHM_SIZE funkce shmctl.

Aplikace produktu IBM MQ MQI client a všechny 64bitové procesy nejsou tímto omezením ovlivněny. Mohou se připojit ke správcům front produktu IBM MQ bez ohledu na to, zda byla nastavena hodnota EXTSHM.

Linux AIX Zdroje pro produkt IBM MQ a UNIX System V IPC

Správce front používá některé prostředky IPC. Použijte **ipcs -a** k vyhledání toho, jaké prostředky se používají.

Tyto informace platí pouze pro IBM MQ spuštěné na systémech AIX and Linux .

IBM MQ používá prostředky IPC (System V interprocess communication) (IPC) (*semafory* a *segmenty sdílené paměti*) k ukládání a předávání dat mezi komponentami systému. Tyto prostředky jsou používány procesy správce front a aplikacemi, které se připojují ke správci front. Produkt IBM MQ MQI clients nepoužívá prostředky IPC, kromě řídicích prvků trasování produktu IBM MQ . Použijte příkaz UNIX **ipcs -a** k získání úplných informací o počtu a velikosti prostředků IPC, které se momentálně používají na počítači.

Linux AIX Priorita procesu IBM MQ a UNIX

Správné postupy při nastavení hodnot priority procesů *nice* .

Tyto informace platí pouze pro IBM MQ spuštěné na systémech AIX and Linux .

Spustíte-li proces na pozadí, může se tento proces dostat do volajícího shellu s vyšší hodnotou *nice* (a tím nižší prioritou). To může mít obecné dopady na výkon produktu IBM MQ . V situacích s vysokou prioritou, pokud existuje mnoho připravených podprocesů s vyšší prioritou a některé s nižší prioritou, mohou charakteristiky plánování operačního systému připravit nižší prioritu podprocesů procesorového času.

Je dobrým zvykem, že nezávisle spuštěné procesy přidružené ke správcům front, jako např. **runmqlsr**, mají stejné hodnoty *nice* jako správce front, ke kterému jsou přidruženy. Ujistěte se, že shell nepřiřazuje těmto procesům na pozadí vyšší hodnotu *nice* . Například v ksh se používá nastavení "`set +o bgnice`" k zastavení ksh ve zvýšení hodnoty *nice* procesů na pozadí. Hodnoty *nice* spuštěných procesů můžete ověřit prohlédnutím sloupce *NI* ve 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 blokovat podproces správce front nebo naopak, který způsobuje snížení výkonu.

z/OS Plánování vašeho prostředí IBM MQ na systému z/OS

Při plánování vašeho prostředí IBM MQ musíte vzít v úvahu požadavky na prostředky pro datové sady, sady stránek, Db2, Prostředky párování a potřebu protokolování a zálohování zařízení. Pomocí tohoto tématu můžete naplánovat prostředí, ve kterém je spuštěn produkt IBM MQ .

Před plánováním architektury produktu IBM MQ se seznamte se základními koncepcemi produktu IBM MQ for z/OS , viz témata v tématu Koncepty produktuIBM MQ for z/OS.

Při plánování správce front může být zapotřebí pracovat s různými osobami ve vaší organizaci. Je obvykle dobrý nápad zapojit tyto lidi brzy, jako procedury řízení změn může trvat dlouhou dobu. Mohou být také schopni říci, jaké parametry potřebujete ke konfiguraci produktu IBM MQ for z/OS.

Například byste mohli potřebovat pracovat s:

- Administrátor úložiště, který určuje vysokoúrovňový kvalifikátor datových sad správce front a přidělil dostatek místa pro datové sady správce front.
- z/OS systémový programátor pro definování subsystému IBM MQ pro z/OS a APF autorizuje knihovny IBM MQ for z/OS .

- Administrátor sítě určuje, 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, profilů zabezpečení pro prostředky produktu IBM MQ for z/OS a certifikátům TLS.
- Administrátor produktu Db2 nastavuje tabulky 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 správce front

Při nastavování správce front by mělo být vašemu plánování umožněno růst správce front, aby správce front splňoval požadavky vašeho podniku.

Nejlepším způsobem, jak nakonfigurovat správce front, je postup:

1. Konfigurace základního správce front
2. Konfigurace inicializátoru kanálu, který provádí komunikaci správce front s komunikací správce front a komunikace vzdálených klientských aplikací
3. Chcete-li šifrovat a chránit zprávy, nakonfigurujte Advanced Message Security
4. Chcete-li použít přenos souborů přes IBM MQ, nakonfigurujte Managed File Transfer pro z/OS.
5. Chcete-li použít administrativní nebo systém zpráv REST APInebo konzolu MQ Console ke správě produktu IBM MQ z webového prohlížeče, nakonfigurujte webový server mqweb.

Některé podniky mají v prostředí tisíce správců front. Nyní je třeba vzít v úvahu síť IBM MQ a za pět let.

V systému z/OSněkteří správci front zpracovávají tisíce zpráv za sekundu a protokol přes 100 MB za sekundu. Pokud očekáváte velmi vysoké objemy dat, budete možná muset zvážit, zda máte více než jednoho správce front.

V produktu z/OSlze produkt IBM MQ spustit jako součást skupiny sdílení front (QSG), kde jsou zprávy uloženy v prostředku Coupling Facility, a každý správce front v rámci skupiny sdílení front může přistupovat ke zprávám. Chcete-li pracovat ve skupině sdílení front, je třeba zvážit počet správců front, které potřebujete. Obvykle existuje jeden správce front pro každou oblast LPAR. Také můžete mít jednoho správce front, který bude zálohovat struktury prostředku CF.

Některé změny v konfiguraci lze snadno provést, jako např. definování nové fronty. Některé jsou složitější, jako např. vytváření protokolů a sad stránek větších; a některé konfigurace nelze změnit, například název správce front nebo název skupiny sdílení front.

V souboru MP16 Performance SupportPac jsou k dispozici informace o výkonu a ladění.

Konvence pojmenování

Pro datové sady správce front je třeba mít konvenci pojmenování.

Mnoho podniků používá číslo vydání v názvu zaváděcích knihoven a tak dále. Možná budete chtít vzít v úvahu alias `MQM.SCSQAUTH` odkazující na aktuálně používanou verzi, například `MQM.V900.SCSQAUTH`, takže při migraci na novou verzi produktu IBM MQnemusíte měnit produkty CICS, Batch a IMS JCL.

V produktu z/OS UNIX System Services můžete použít symbolický odkaz, který bude odkazovat na instalační adresář pro aktuálně používanou verzi produktu IBM MQ .

Datové sady použité správcem front (protokoly, sady stránek, knihovny JCL) potřebují konvenci pojmenování pro zjednodušení vytváření profilů zabezpečení a mapování datových sad do paměťových tříd SMS, které řídí umístění datových sad na disk, a atributy, které mají.

Všimněte si, že vložení verze produktu IBM MQ do názvu sady stránek nebo protokolů, není dobrý nápad. Jednoho dne můžete provést migraci na novou verzi a datová sada bude mít názvy "nesprávné".

Aplikace

Musíte porozumět obchodním aplikacím a nejlepším způsobem, jak nakonfigurovat produkt IBM MQ. Pokud mají aplikace například logiku pro poskytování zotavení a opakování, mohou být netrvalé zprávy dostačující. Pokud chcete, aby produkt IBM MQ ošetložil obnovu, musíte použít trvalé zprávy a vložit a načíst zprávy v synchronizačním bodu.

Je třeba izolovat fronty od různých obchodních transakcí. Pokud se zaplnění fronty pro jednu obchodní aplikaci zaplní, nechcete mít dopad na ostatní obchodní aplikace. Je-li to možné, izolujte fronty v různých sadách stránek a fondech vyrovnávacích pamětí, případně struktury.

Je třeba porozumět profilu zpráv. Pro mnoho aplikací mají fronty pouze několik zpráv. Ostatní aplikace mohou mít v průběhu dne sestavení front a budou zpracovány přes noc. Fronta, která má v sobě za normálních okolností pouze několik zpráv, může vyžadovat uchování zpráv o počtu hodin v případě, že se nevyskytl problém a zprávy nejsou zpracovány. Je třeba nastavit velikost struktur a sad stránek prostředku CF, aby bylo možné dosáhnout očekávané maximální kapacity.

Konfigurace po konfiguraci

Jakmile jste nakonfigurovali správce front (a komponenty), musíte plánovat:

- Zálohování sad stránek.
- Zálohování definic objektů.
- Automatizuje zálohování všech struktur CF.
- Monitorování zpráv produktu IBM MQ a provedení akce, pokud je zjištěn problém.
- Shromažďování statistických dat produktu IBM MQ .
- Monitorování využití prostředků, jako je například virtuální úložiště, a množství dat protokolovaných za hodinu. Pomocí této akce můžete zjistit, zda se vaše využití prostředků zvyšuje a zda je třeba provést určité akce, jako je nastavení nového správce front.

z/OS Plánování vašeho úložiště a požadavků na výkon v systému z/OS

Musíte nastavit realistické a dosažitelné úložiště a výkonnostní cíle pro váš systém IBM MQ . Toto téma vám pomůže porozumět faktorům, které ovlivňují úložiště, a výkon.

Toto téma obsahuje informace o požadavcích na úložiště a výkon produktu IBM MQ for z/OS. Obsahuje následující oddíly:

- z/OS volby výkonu pro IBM MQ
- Určení důležitosti správy pracovní zátěže z/OS a cílů rychlosti
- “Úložiště knihovny” na stránce 144
- “Použití LX systému” na stránce 144
- “Paměť adresního prostoru” na stránce 145
- “Disková paměť” na stránce 149

Další informace viz “Kde najdete další informace o požadavcích na úložiště a výkon” na stránce 149 .

Volby výkonu produktu z/OS pro produkt IBM MQ

Pomocí správy pracovní zátěže definujete cíle výkonu a přiřazujete jednotlivým cílům obchodní důležitost. Můžete definovat cíle pro práci v obchodních termínech a systém rozhodne o tom, kolik prostředků, jako je

procesor a úložiště, by mělo být poskytnuto k práci, aby splnil svůj cíl. Správa pracovní zátěže řídí prioritu odbavení na základě cílů, které jste zadali. Správa pracovní zátěže zvyšuje nebo snižuje prioritu podle potřeby tak, aby vyhovovala zadanému cíli. Proto nemusíte finàta vyladit přesné priority každého kusu práce v systému a místo toho se můžete soustředit na obchodní cíle.

K dispozici jsou tři druhy cílů:

Doba odezvy
Jak rychle chcete, aby práce byla zpracována

Rychlost provedení
Jak rychle by měla být práce spouštěna, když je připravena, aniž by byla odložena na procesor, paměť, I/O přístup a zpoždění fronty

diskreční
Kategorie pro práci s nízkou prioritou, pro kterou neexistují žádné výkonnostní cíle

Cíle doby odezvy jsou vhodné pro aplikace koncového uživatele. Uživatelé produktu CICS mohou například nastavit cíle pracovní zátěže jako cíle doby odezvy. Pro adresní prostory portálu IBM MQ jsou cíle rychlosti vhodnější. Do tohoto cíle rychlosti se započítává malé množství práce vykonané ve správci front, ale tato práce je kritická pro výkon. Většina práce, kterou provádí správce front, se započítává do cíle výkonu aplikace koncového uživatele. Většina práce, kterou provádí adresní prostor iniciátoru kanálu, se počítá směrem k vlastnímu cíli rychlosti. Příjem a odesílání zpráv produktu IBM MQ , které iniciátor kanálu provádí, je obvykle důležité pro výkon obchodních aplikací, které je používají.

Určení důležitosti správy pracovní zátěže produktu z/OS a cílů rychlosti

Další informace viz “Určení důležitosti správy pracovní zátěže produktu z/OS” na stránce 144.

Úložiště knihovny

V 9.2.0 Musíte přidělit diskovou paměť pro knihovny produktu. Přesné údaje závisejí na vaší konfiguraci a měly by obsahovat jak cílové, tak distribuční knihovny, stejně tak 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 velikostech a požadovaném formátu najdete v adresáři programu. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Použití LX systému

Každý definovaný subsystém IBM MQ rezervuje jeden index propojení systému (LX) v době IPL a počet indexů připojení mimo systém, když je správce front spuštěn. Systémový sestavovací index se znovu použije při zastavení a restartu správce front. Podobně distribuovaná fronta rezervuje jeden index sestavení mimo systém. V nepravděpodobném případě vašeho systému z/OS s neadekvátním systémem LXs je možné, že budete muset vzít tyto vyhrazené systémové hodnoty LXs na účet.

Je-li to nutné, může být počet LXů systému zvýšen nastavením parametru *NSYSLX* v 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 *Paměť adresního prostoru*

Toto téma obsahuje základní pokyny týkající se požadavků na adresní prostor pro komponenty produktu IBM MQ .

Požadavky na úložný prostor lze rozdělit do následujících kategorií:

- Společné úložiště
- Využití úložiště soukromého regionu správce front
- Použití úložiště inicializátoru kanálu

V 64bitovém adresovém prostoru se nachází virtuální linka s názvem "panel" , která označuje adresu 2GB . Panel odděluje úložiště pod adresou 2GB pod názvem "pod pruhem", od úložiště nad adresou 2GB , která se nazývá "nad pruhem". Úložiště pod pruhem používá 31bitovou adresovatelnost, úložný prostor nad barem používá 64bitovou adresovatelnost.

Limit 31bitového úložiště můžete určit pomocí parametru REGION v souboru JCL a omezením nad úložným prostorem pomocí parametru MEMLIMIT. Tyto zadané hodnoty lze přepsat pomocí ukončení MVS .

Upozornění: Byla zavedena změna způsobu práce systému. Nyní, Cross-system Extended Services (XES) přidělí 4GB úložiště ve vysokém virtuálním úložišti pro každé připojení ke serializované struktuře seznamu.

Před touto změnou byla tato paměť přidělena v datových prostorech. Po použití této opravy APAR na základě způsobu, jakým IBM MQ vypočítá využití úložiště, může být vydána zpráva CSQY225E a CSQY224I , což indikuje, že `správce front je příliš krátký na místní paměti nad pruhem`.

Uvidíte také zvýšení nad výše uvedenými sloupcovými hodnotami ve zprávě CSQY220I

Další informace najdete v dokumentu podpory společnosti IBM 2017139.

Navrhované velikosti regionů

Následující tabulka zobrazuje doporučené hodnoty pro velikosti regionů.

Tabulka 19. Doporučené definice pro velikosti oblastí JCL

Nastavení definice	**Systém**
Správce front	REGION=0M, MEMLIMIT=3G
Inicializátor kanálu	REGION=0M

Společné úložiště

Každý subsystém IBM MQ for z/OS má následující přibližné požadavky na úložiště:

- CSA 4KB
- ECSA 800KBplus velikost tabulky trasování, která je uvedená v parametru TRACTBL makra CSQ6SYSP systémového parametru. Další informace najdete v tématu Použití CSQ6SYSP.

Kromě toho každé souběžné logické připojení IBM MQ vyžaduje přibližně 5 KB systému ECSA. Když je úloha ukončena, jiné úlohy IBM MQ mohou toto úložiště znovu použít. Produkt IBM MQ neuvolní paměť, dokud není správce front vypnutý, takže můžete vypočítat maximální množství požadované ECSA vynásobením maximálního počtu souběžných logických připojení hodnotou 5KB. Počet souběžných logických připojení je součtem počtu:

- Úlohy (TCB) v oblastech dávkových úloh, TSO, z/OS UNIX System Services, IMSa Db2 (SPAS), které jsou připojené k produktu IBM MQ, ale nejsou odpojeny.
- Transakce CICS , které vydaly požadavek IBM MQ , ale nebyly ukončeny
- JMS Connections, Sessions, TopicSessions nebo QueueSessions , které byly vytvořeny (pro připojení vazeb), ale dosud nebyly zničeny, nebo byly vyčištěné.
- Aktivní kanály produktu IBM MQ .

Můžete nastavit omezení na společné úložiště použité logickými připojeními ke správci front pomocí konfiguračního parametru ACELIM. Ovládací prvek ACELIM je primárně zaměřen na weby, ve kterých uložené procedury produktu Db2 způsobují operace ve frontách produktu IBM MQ .

Při použití uložené procedury může každá operace produktu IBM MQ vést k novému logickému připojení ke správci front. Velké jednotky práce Db2 , například z důvodu načtení tabulky, mohou vést k nadměrné poptávce po společném úložišti.

ACELIM je určen k omezení běžného ukládání dat a k ochraně systému z/OS tím, že omezuje počet připojení v systému. Měla by být nastavena pouze na správce front, kteří byli identifikováni jako použití nadměrného množství paměti ECSA. Další informace naleznete v sekci ACELIM v části Použití CSQ6SYSP .

Chcete-li nastavit hodnotu parametru ACELIM, nejprve určete množství paměti, které je aktuálně v podfondu řízených hodnotou ACELIM. Tyto informace se nacházejí v záznamech SMF 115 podtypu 5, které byly vytvořeny trasováním třídy CLASS (3).

IBM MQ Data SMF mohou být formátována pomocí balíku SupportPac MP1B. Počet bajtů používaných v podfondu řízeném pomocí 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.

Zvyšte běžnou hodnotu o dostatečné ziskové rozpětí, abyste zajistili prostor pro růst a špičky pracovní zátěže. Vydělte novou hodnotu o 1024, aby se v konfiguraci ACELIM použila maximální velikost úložiště v kB pro použití.

Inicializátor kanálu obvykle vyžaduje použití ECSA až 160KB.

Využití úložiště soukromého regionu správce front

Produkt IBM MQ for z/OS může používat úložiště nad 2GB barem pro některé vnitřní řídicí bloky. V této paměti můžete mít fondy vyrovnávacích pamětí, které vám poskytují možnost nakonfigurovat mnohem větší fondy vyrovnávacích pamětí, je-li k dispozici dostatečné úložiště. Běžně jsou fondy vyrovnávacích pamětí hlavní vnitřní řídicí bloky, které využívají úložiště nad panelem 2GB .

Každá velikost fondu vyrovnávacích pamětí je určena v době inicializace správce front a je alokována pro fond vyrovnávacích pamětí, když je připojena sada stránek, která používá daný fond vyrovnávacích pamětí. Nový parametr LOCATION (NAD | BELOW) se používá k určení místa, kde jsou vyrovnávací paměti alokovány. Příkaz ALTER BUFFPOOL můžete použít k dynamické změně velikosti fondů vyrovnávacích pamětí.

Chcete-li použít nad pruhem (64 bit) paměti, můžete zadat hodnotu parametru MEGIMIT (například MEMLIMIT=3G) na parametru **EXEC PGM=CSQYASCP** v JCL správce front. Vaše instalace může mít výchozí sadu hodnot.

Měli byste uvést MEMLIMIT a uvést rozumnou velikost úložiště, spíše než MEVIMIT = NOLIMIT, abyste předešli možným problémům. Uvedete-li NOLIMIT nebo velmi velkou hodnotu, pak příkaz ALTER BUFFPOOL s velkou velikostí může použít všechny dostupné virtuální úložiště z/OS , které povede k stránkování ve vašem systému. Je možné, že budete potřebovat diskutovat o hodnotě MEGIMIT se systémovým programátorem produktu z/OS , v případě, že existuje celosystémový limit množství paměti, které lze použít.

Začněte s parametrem MEMLIMIT=3G a zvyšte tuto velikost, když potřebujete zvýšit velikost fondů vyrovnávacích pamětí.

Vypočítejte hodnotu parametru MEMLIMIT jako 2GB a velikost fondů vyrovnávacích pamětí nad sloupec zaokrouhlenou na nejbližší GB. Nastavte MEMMLIMIT na minimum 3GBa podle potřeby jej zvyšte, pokud potřebujete zvýšit velikost vašich fondů vyrovnávacích pamětí.

Například pro 2 fondy vyrovnávacích pamětí konfigurované s UMÍSTĚNÍ má fond vyrovnávacích pamětí 1 10 000 vyrovnávacích pamětí, fond vyrovnávacích pamětí 2 má 50 000 vyrovnávacích pamětí. Využití paměti nad sloupcem se rovná 60 000 (celkový počet vyrovnávacích pamětí) * 4096 = 245,760,000 bajtů = 234.375MB. Všechny fondy vyrovnávacích pamětí bez ohledu na LOCATION budou využívat 64 bitového úložiště pro řídicí struktury. Počet fondů vyrovnávacích pamětí a počet vyrovnávacích pamětí v těchto fondech se může stát významným zvýšením. Každá vyrovnávací paměť vyžaduje přibližně dalších 200 bajtů paměti 64bitového úložiště. Pro konfiguraci s 10 fondy vyrovnávacích pamětí každá s 20 000 vyrovnávacích pamětí, která by vyžadovala: 200 * 10 * 20 000 = 40,000.000, což odpovídá 40MB. Můžete uvést 3GB pro velikost MEVIMIT, která umožní rozsah růstu (40MB + 200MB + 2GB , což zaokrouhlí nahoru na 3GB).

Pro některé konfigurace může existovat významný výkonnostní přínos pro použití vyrovnávacích pamětí, které mají své vyrovnávací paměti trvale zálohované skutečným úložištěm. Toho lze dosáhnout uvedením hodnoty FIXED4KB pro atribut PAGECLAS fondu vyrovnávacích pamětí. Tuto operaci byste však měli provést pouze v případě, je-li v logické oblasti k dispozici dostatek reálné paměti, jinak by mohly být ovlivněny jiné adresní prostory. Informace o tom, kdy byste měli použít hodnotu FIXED4KB pro PAGECLAS, najdete v tématu IBM MQ Support Pac MP16: IBM MQ for z/OS -Plánování kapacity a ladění

Před použitím paměti nad pruhem byste měli prodiskutovat se svými systémovými programátory z/OS , abyste se ujistili, že je k dispozici dostatek pomocné paměti pro maximální využití času a dostatečné požadavky na skutečné úložiště pro zabránění stránkování.

Poznámka: Je možné, že bude třeba zvýšit velikost datových sad výpisu paměti, aby bylo možné dosáhnout vyššího virtuálního úložiště.

Velikost fondu vyrovnávacích pamětí tak velká, že může dojít ke stránkování MVS , může negativně ovlivnit výkon. Můžete zvážit použití menšího fondu vyrovnávacích pamětí, který nestránkue, s IBM MQ přesunutím zprávy do sady stránek a ze sady stránek.

Využití úložiště adresního prostoru můžete monitorovat ze zprávy CSQY220I, které označuje velikost úložiště soukromého regionu ve výše a pod pruhem 2GB a zbývající množství.

Využití úložiště inicializátoru kanálu

Existují dvě oblasti použití úložiště inicializátoru kanálu, které musíte vzít v úvahu:

- Soukromá oblast
- Účetnictví a statistika

Použití úložiště v soukromém regionu

Pro parametr CHINIT byste měli zadat REGION=0M , aby bylo možné použít maximum pod pruhem úložiště. Paměť dostupná pro iniciátor kanálu omezuje počet souběžných připojení, které může CHINIT mít.

Každý kanál používá přibližně 170KB přídavného soukromého regionu v adresovém prostoru inicializátoru kanálu. Pokud jsou zprávy větší než 32KB přenášeny, je velikost zprávy zvětšena o velikost zprávy. Tato zvýšená paměť se uvolní, když:

- Odesílající nebo kanál klienta vyžaduje méně než polovinu aktuální velikosti vyrovnávací paměti pro 10 následných zpráv.
- Prezenční signál je odeslán nebo přijat.

Úložiště je uvolněno pro opětovné použití v rámci jazykového prostředí, avšak správce virtuálního úložiště produktu z/OS jej nevnímá jako volné. To znamená, že horní limit počtu kanálů je závislý na velikosti zpráv a ve vzorech příjmu a na omezeních jednotlivých uživatelských systémů na rozšířené velikosti soukromého regionu. Horní limit počtu kanálů bude pravděpodobně v mnoha systémech přibližně 9000, protože velikost rozšířeného regionu pravděpodobně nepřekročí 1.6GB. Použití velikostí zpráv větších než 32KB snižuje maximální počet kanálů v systému. Například, pokud jsou přeneseny zprávy 100MB a předpokládá se velikost rozšířeného regionu 1.6GB , maximální počet kanálů je 15.

Trasování inicializátoru kanálu je zapsáno do datového prostoru. Velikost paměti datového prostoru je řízena parametrem **TRAXTBL** . Viz ALTER QMGR.

Evidence a statistika využití paměti

Měli byste povolit přístup inicializátoru kanálu alespoň k 256MB virtuálního úložiště nad panelem. To můžete provést uvedením `MEMLIMIT=256M`.

Pokud nenastavíte parametr MEMLIMIT v JCL inicializátoru kanálu, můžete nastavit velikost virtuálního úložiště nad sloupcem pomocí parametru MOMMLIMIT v členu SMFPRMxx SYS1.PARMLIB, nebo z uživatelské procedury IEFUSI.

Pokud nastavíte parametr MEMLIMIT tak, aby omezoval vyšší než požadovanou úroveň úložiště, vydá inicializátor kanálu zprávu CSQX124E a nebude k dispozici evidence evidence a sledování statistiky třídy 4.

Správa velikosti MEMMLIMIT a REGION

Další mechanizmy, například parametr **MEMLIMIT** ve členu SMFPRMxx operačního systému SYS1.PARMLIB nebo IEFUSI exit lze použít ve vaší instalaci k poskytnutí výchozího množství virtuálního úložiště nad řádkem pro adresní prostory z/OS . V části Správa paměti nad pruhem najdete podrobné informace o omezení velikosti úložiště nad pruhem.

Statistika SMDS (Shared Message Data Set) a MIMMLIMIT

Při spuštění pracovní zátěže systému zpráv s použitím sdílených datových sad zpráv existují dvě úrovně optimalizace, kterých lze dosáhnout úpravou atributů DSBUFS a DSBLOCK.

Velikost výše uvedeného úložiště správce front používaného pro vyrovnávací paměť SMDS je DSBUFS x DSBLOCK. To znamená, že hodnota 100 x 256KB (25MB) se standardně používá pro každou strukturu CFLEVEL (5) ve správci front.

Přestože tato hodnota není příliš vysoká, pokud váš podnik nebo podniky mají mnoho CFSTRUCT, některé z nich mohou přidělit vysokou hodnotu MEGIMIT pro fondy vyrovnávacích pamětí a někdy mají také hluboké indexované fronty, takže celkem mohou mít nedostatek prostoru pro ukládání nad panelem.

z/OS *Disková paměť*

Toto téma se používá při plánování požadavků na diskové úložiště pro datové sady protokolů, úložiště Db2 , úložiště prostředku Coupling Facility a datové sady stránek.

Spolupracujte s administrátorem úložiště, abyste určili, kam umístit datové sady správce front. Váš administrátor ukládání může například poskytnout vám určité svazky DASD nebo třídy úložiště SMS, datové třídy a třídy správy pro různé typy datových sad.

- Datová sada protokolu musí být na DASD. Tyto protokoly mohou mít vysokou aktivitu vstupu/výstupu s malou dobou odezvy a nemusí být zálohovány.
- Archivní protokoly mohou být na DASD nebo na pásce. Po jejich vytvoření již nemusí být nikdy znovu načteny s výjimkou abnormální situace, jako je obnova sady stránek ze zálohy. Měly by mít dlouhé datum uchování.
- Sady stránek mohou být nízké až střední aktivity a měly by být pravidelně zálohovány. U systému s vysokým využitím by měly být zálohovány dvakrát denně.
- BSDS datové sady 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.

Prohlédněte si následující sekce, abyste získali podrobnosti o tom, jak plánovat datové úložiště:

- **Protokoly a archivní paměť**

  Část “Jak dlouho budu muset uchovávat protokoly archivace” na stránce 166 popisuje, jak určit, kolik paměťového prostoru potřebuje vaše aktivní protokol a archivní datové sady, v závislosti na objemu zpráv, které zpracovává váš systém IBM MQ a jak často jsou aktivní protokoly odloženy do vašich datových sad archivu.
- **Db2 paměť**

  Část “Db2 úložný prostor” na stránce 183 popisuje, jak určit, jaké množství paměti Db2 vyžaduje pro data IBM MQ .
- **úložiště prostředku Coupling Facility**

  Část “Definování prostředků prostředku Coupling Facility” na stránce 174 popisuje, jak zjistit, jak velký se má vaše struktura prostředku Coupling Facility provádět.
- **Sada stránek a úložiště zpráv**

  Část “Plánování sad stránek a fondů vyrovnávacích pamětí” na stránce 150 popisuje, jak určit, kolik úložiště vyžadují vaše datové sady stránek, v závislosti na velikosti zpráv, které vaše aplikace vyměňují, na číslech těchto zpráv a na rychlosti, jakou jsou vytvářeny nebo vyměňovány.

z/OS *Kde najdete další informace o požadavcích na úložiště a výkon*

Toto téma použijte jako referenci k vyhledání dalších informací o požadavcích na úložiště a výkon.

Další informace můžete najít z následujících zdrojů:

Tabulka 20. Kde najdete další informace o požadavcích na úložiště

Téma	**Kde hledat**
Parametry systému	Použití CSQ6SYSP a Úprava správců front
Úložiště vyžadované k instalaci produktu IBM MQ	Adresář programu. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Tabulka 20. Kde najdete další informace o požadavcích na úložiště (pokračování)	
Téma	**Kde hledat**
IEALIMIT a IEFUSI ukončuji	*Uživatelské procedury instalace MVS*, dostupné na webu zSeries z/OS Internetová knihovna.
Nejnovější informace	Webový server IBM MQ 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 čísla a velikostí datových sad stránek a fondů vyrovnávacích pamětí.

Toto téma obsahuje následující sekce:

Plánování sad stránek

Využití sady stránek

U zpráv s krátkou životností se na sadě stránek obvykle používá málo stránek a v datových sadách je málo nebo žádný vstup/výstup s výjimkou spuštění, během kontrolního bodu nebo při ukončení práce systému.

U dlouhých zpráv s životností jsou tyto stránky, které obsahují zprávy, obvykle zapisovány na disk. Tato operace je prováděna správcem front za účelem zkrácení doby restartování.

Oddělte krátkodobé zprávy od dlouhotrvačných zpráv tím, že je umístíte na různé sady 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, takže mapování front na sady stránek je jednodušší.

Použití více menších sad stránek má řadu výhod. Například trvá méně času zálohování a I/O lze provádět paralelně během zálohování a znovuspuštění. Zvažte však to, že se jedná o významné zvýšení výkonu pro roli administrátora produktu IBM MQ , který je nezbytný k mapování každé fronty na jeden z mnohem většího počtu sad stránek.

Definujte alespoň pět sad stránek následujícím způsobem:

- Sada stránek vyhrazená pro definice objektů (sada stránek nula)
- Sada stránek pro zprávy související s systémem
- Sada stránek pro zprávy s dlouhou životností kritické pro výkon
- Sada stránek pro krátkodobé prožité zprávy s kritickým výkonem
- Sada stránek pro všechny ostatní zprávy

"Definování vašich fondů vyrovnávacích pamětí" na stránce 155 vysvětluje výkonnostní výhody při distribuci vašich zpráv na sadách stránek tímto způsobem.

Velikost sad stránek

Nadefinujte dostatečný prostor ve vašich sadách stránek pro očekávanou maximální kapacitu zpráv. Zvažte případné neočekávané maximální kapacity, jako je například sestavení zpráv, které se vyvíjejí, protože program fronty není spuštěn. To lze provést přidělením sady stránek se sekundárními oblastmi nebo alternativně povolením rozšíření dynamické sady stránek. Další informace viz téma "Povolení rozšíření dynamické sady stránek" na stránce 153. Je obtížné nastavit sadu stránek menší, takže je často lepší přidělit menší sadu stránek a umožnit její rozbalení podle potřeby.

Při plánování velikosti sad stránek zvažte všechny zprávy, které mohou být generovány, včetně dat neaplikačních zpráv. Například, zprávy spouštěče, zprávy událostí a všechny zprávy sestavy, které vaše aplikace požadovala.

Velikost sady stránek určuje čas potřebný k obnovení sady stránek při obnovování ze zálohy, protože větší sada stránek trvá déle, než je obnova.

Poznámka: Obnovení sady stránek závisí také na době, kdy správce front trvá zpracovat záznamy protokolu zapsané od doby provedení zálohy; toto časové období je určeno frekvencí zálohování. Další informace viz téma "Plánování zálohování a obnovy" na stránce 185.

Poznámka: Sady stránek větší než 4 GB vyžadují použití rozšířené adresovatelnosti SMS.

V 9.2.0 **Plánování šifrování datové sady produktu z/OS**

Funkci šifrování datové sady produktu z/OS lze použít na sady stránek pro správce front spuštěné v produktu IBM MQ for z/OS 9.1.4 nebo pozdější.

Tyto sady stránek je třeba přidělit spolu s atributy EXTENDED a popisek klíče datové sady, který zajišťuje, že jsou data šifrována pomocí AES.

Informace naleznete v části Důvěrnost dat v produktu IBM MQ for z/OS s šifrováním datové sady. Další informace viz.

Vypočítejte velikost vašich sad stránek

Pro definice objektů správce front (například fronty a procesy) je jednoduché vypočítat požadavek na úložiště, protože tyto objekty mají pevnou velikost a jsou trvalé. Pro zprávy je však výpočet složitější z následujících důvodů:

- Velikost zpráv se liší.
- Zprávy jsou přechodné.
- Prostor zabíraný zprávami, které byly načteny, jsou pravidelně uvolňovány asynchronním procesem.

Velké sady stránek větší než 4 GB, které poskytují dodatečnou kapacitu pro zprávy v případě, že se síť zastaví, lze vytvořit, je-li to nutné. Existující sady stránek není možné upravit. Místo toho musí být vytvořeny nové sady stránek s rozšířenými addressmability a atributy rozšířeného formátu. Nové sady stránek musí být stejné fyzické velikosti jako staré a staré sady stránek musí být zkopírovány do nových sad stránek. Je-li vyžadována zpětná migrace, nesmí být změněna sada stránek nula. Pokud jsou sady stránek menší než 4 GB dostatečné, není třeba žádná akce.

Sada stránek nula

Nulová stránka sady stránek je vyhrazena pro definice objektů.

Pro sadu stránek nula 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)
```

Vydělte tuto hodnotu hodnotou 4096, abyste určili počet záznamů, které mají být zadány v klastru pro datovou sadu sady stránek.

Nemusíte povolit objekty uložené ve sdíleném úložišti, ale musíte povolit objekty, které jsou uloženy nebo zkopírovány na stránku 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 paměť požadovaná pro každou sadu stránek určena počtem a velikostí zpráv uložených na dané sadě stránek. (Zprávy ve sdílených frontách se neukládají do sad stránek.)

Vydělte tuto hodnotu hodnotou 4096, abyste určili počet záznamů, které mají být zadány v klastru pro datovou sadu sady stránek.

Výpočet požadavku úložiště pro zprávy

Tento oddíl popisuje, jak jsou zprávy ukládány na stránky. Porozumění této možnosti vám pomůže vypočítat, kolik prostoru pro ukládání stránek musíte definovat pro vaše zprávy. Chcete-li vypočítat přibližný prostor vyžadovaný pro všechny zprávy na sadě stránek, musíte zvážit maximální hloubku fronty všech front, které jsou mapovány na danou sadu stránek, a průměrnou velikost zpráv v těchto frontách.

Poznámka: Velikosti struktur a řídicích informací uvedených v tomto oddílu se mohou měnit mezi hlavními verzemi. Podrobnosti specifické pro vaši verzi produktu IBM MQnajdete v části SupportPac MP16 - WebSphere MQ pro z/OS Plánování kapacity & ladění a IBM MQ Sestavy výkonu

Musíte povolit možnost, že zpráva "gets" může být zpožděna z důvodů mimo ovládací prvek IBM MQ (například kvůli problému s komunikačním protokolem). V takovém případě může rychlost "put" zpráv daleko překročit rychlost "get". To může vést k velkému zvýšení počtu zpráv uložených v sadě stránek a následnému zvýšení požadované velikosti úložiště.

Každá stránka v sadě stránek je dlouhá 4096 bajtů. Povolíte-li informace o pevném záhlaví, každá stránka má k dispozici 4057 bajtů prostoru pro ukládání zpráv.

Při výpočtu požadovaného prostoru pro každou zprávu je první věc, kterou musíte 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 reprezentována následujícím způsobem:

Část záhlaví zprávy obsahuje deskriptor zprávy a další řídicí informace, jejichž velikost se liší v závislosti na velikosti zprávy. Část dat zprávy obsahuje všechna skutečná data zprávy a jakákoli další záhlaví (například záhlaví přenosu nebo záhlaví mostu IMS).

Pro řídicí informace sady stránek se požadují minimálně dvě stránky, které jsou typicky méně než 1% z celkového prostoru potřebného pro zprávy.

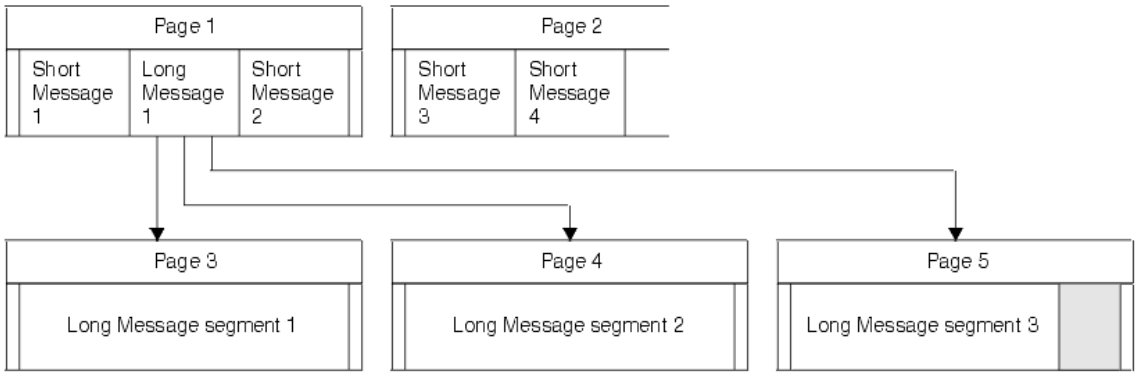
Krátké zprávy

Krátká zpráva je definována jako zpráva, která se vejde na jednu stránku.

V produktu IBM WebSphere MQ 7.0.1jsou malé zprávy uloženy na každé stránce jedna.

Dlouhé zprávy

Pokud je velikost dat zprávy větší než 3596 bajtů, ale není větší než 4 MB, bude zpráva klasifikována jako dlouhá zpráva. Při zobrazení dlouhé zprávy produkt IBM MQ ukládá zprávu na řadu stránek a ukládá řídicí informace, které ukazují na tyto stránky stejným způsobem, jako by ukládala krátkou zprávu. To je zobrazeno v souboru Obrázek 41 na stránce 153:



Obrázek 41. Jak produkt IBM MQ ukládá dlouhé zprávy na sadách stránek

Velmi dlouhé zprávy

Velmi dlouhé zprávy jsou zprávy o velikosti větší než 4 MB. Ty jsou uloženy tak, aby každá 4 MB používala 1037 stránek. Jakýkoli zůstatek je uložen stejným způsobem jako dlouhá zpráva, jak je popsáno výše.

z/OS *Povolení rozšíření dynamické sady stránek*

Sady stránek lze dynamicky rozšiřovat, zatímco je správce front spuštěn. Sada stránek může mít 123 oblastí a může být rozložena na více diskových svazků.

Při každém rozbalení sady stránek se použije nová oblast datové sady. Správce front dále rozbalí sadu stránek podle potřeby, dokud není dosaženo maximálního počtu oblastí pro rozšíření nebo dokud není k dispozici více úložišť pro přidělení na vhodných svazcích.

Jakmile se expanze sady stránek nezdaří z některého z důvodů uvedených výše, správce front označí stránku nastavenou pro žádné další pokusy o rozšíření. Toto označení může být resetováno změnou nastavení stránky na EXPAND (SYSTEM).

Expanze sady stránek probíhá asynchronně na všechny ostatní aktivity sady stránek, když je přiděleno 90% existujícího prostoru v sadě stránek.

Rozšiřující proces sady stránek formátuje nově alokovaný rozsah a zpřístupní jej pro použití správcem front. Nicméně žádný prostor není k dispozici pro použití, dokud není zformátován celý rozsah. To znamená, že expanze do velké míry bude pravděpodobně nějakou dobu trvat a aplikace mohou 'blokovat', pokud naplní zbývajících 10% sady stránek ještě před dokončením rozbalení.

Ukázka thlqual.SCSQPROC(CSQ4PAGE) ukazuje, jak definovat sekundární oblasti pro rozšíření.

Chcete-li určit velikost nových oblastí pro rozšíření, použijte jednu z následujících možností modulu EXPAND příkazů DEFINE PSID a ALTER PSID:

- UŽIVATEL
- SYSTÉM
- ŽÁDNÉ

UŽIVATEL

Používá velikost sekundární oblasti pro rozšíření, která byla zadána při alokaci sady stránek. Pokud hodnota nebyla uvedena, nebo pokud byla zadána hodnota nula, nemůže dojít k rozšíření dynamické sady stránek.

Rozšíření sady stránek se objevuje, když je prostor na stránce 90% používán a je prováděn asynchronně s jinou aktivitou sady stránek.

To může vést k rozšíření o více než jednu fyzickou oblast v daném okamžiku.

Podívejte se na následující příklad: přidělíte sadu stránek s primární oblastí 100.000 stránek a sekundárním rozsahem 5000 stránek. Je vložena zpráva, která vyžaduje 9999 stránek. Pokud sada stránek již používá 85000 stránek, zápis zprávy překračuje hranici 90% (90 000 stránek). V tomto bodě je další sekundární fyzická oblast přidělena do primárního rozsahu 100 000 stránek, přičemž velikost stránky bude nastavena na 105,000 stránek. Zbývajících 4999 stran zprávy pokračuje v zápisu. Když využitý prostor stránky dosáhne 94.500 stránek, což je 90% aktualizované velikosti stránky 105.000 stránek, alokuje se dalších 5000 stránek 5000 stránek, přičemž velikost stránky nastaví velikost na 110 000 stránek. Na konci MQPUT se sada stránek rozšířila dvakrát a použijí se 94.500 stránek. Nebyla použita žádná stránka v druhém rozšíření sady stránek, ačkoli byla alokována.

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 uvedena, když byla definována sada stránek. Místo toho správce front nastaví hodnotu, která bude přibližně 10% aktuální velikosti sady stránek. Hodnota je zaokrouhlena nahoru na nejbližší cylindr DASD.

Pokud nebyla uvedena hodnota, nebo pokud byla zadána hodnota nula, může se expanze dynamické sady stránek stále vyskytnout. Správce front nastaví hodnotu, která bude přibližně 10% aktuální velikosti sady stránek. Nová hodnota se zaokrouhluje nahoru v závislosti na charakteristice DASD.

Rozšíření sady stránek se vyskytne, když je prostor v sadě stránek přibližně 90% používán, a je prováděn asynchronně s jinou aktivitou 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

K provedení další expanze sady stránek již není zapotřebí žádné další rozšíření.

Související odkazy
POZMĚNIT PSID
DEFINOVAT PSID
Zobrazení využití

Definování vašich 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 částí:

Rozhodněte se o počtu fondů vyrovnávacích pamětí, které chcete definovat

Měli byste nejprve definovat čtyři fondy vyrovnávacích pamětí:

Fond vyrovnávacích pamětí 0
Použijte pro definice objektů (v sadě stránek nula) a kritické výsledky, fronty zpráv související se systémem, jako např. SYSTEM.CHANNEL.SYNCQ a SYSTEM.CLUSTER.COMMAND.QUEUE a SYSTEM.CLUSTER.REPOSITORY.QUEUE fronty.

Je však důležité zvážit použití bodu "7" na stránce 157 v části *Upravit charakteristiky fondu vyrovnávacích pamětí* , pokud má být použit velký počet kanálů nebo klastrování.

Pro zprávy uživatele použijte zbývající tři fondy vyrovnávacích pamětí.

Fond vyrovnávacích pamětí 1
Použití pro důležité dlouhotrvaly zprávy.

Dlouholeté zprávy jsou zprávy, které zůstanou v systému déle než dva kontrolní body, kdy jsou zapsány do této sady stránek. Pokud máte mnoho zpráv s dlouhou životností, měl by být tento fond vyrovnávacích pamětí relativně malý, takže I/O sada stránek je rovnoměrně distribuována (starší zprávy se zapíší do DASD pokaždé, kdy se fond vyrovnávacích pamětí zaplní o 85%).

Je-li fond vyrovnávacích pamětí příliš velký a fond vyrovnávacích pamětí se nikdy nedostane do 85% plného, stránková sada I/O je odložena až do zpracování kontrolního bodu. To může ovlivnit doby odezvy v celém systému.

Pokud očekáváte pouze několik zpráv s dlouhou životností, definujte tento fond vyrovnávacích pamětí tak, aby byl dostatečně velký, aby mohl obsahovat všechny tyto zprávy.

Fond vyrovnávacích pamětí 2
Použijte pro kritické zprávy s krátkodobou životností.

Obvykle existuje vysoký stupeň opětovného použití vyrovnávací paměti pomocí několika vyrovnávacích pamětí. Tento fond vyrovnávacích pamětí byste však měli tento fond vyrovnávacích pamětí vytvořit tak, aby umožňoval neočekávanou akumulaci zpráv, například když selže serverová aplikace.

Fond vyrovnávacích pamětí 3
Používá se pro všechny ostatní (obvykle výkonové nekritické) zprávy.

Fronty, jako je fronta nedoručených zpráv, SYSTEM.COMMAND* fronty a SYSTEM.ADMIN.* Fronty mohou být také mapovány do fondu vyrovnávacích pamětí 3.

Pokud existují omezení virtuálního úložiště a fondy vyrovnávacích pamětí musí být menší, fond vyrovnávacích pamětí 3 je prvním kandidátem na zmenšení velikosti.

Možná budete muset definovat další fondy vyrovnávacích pamětí za následujících okolností:

- Je-li o určité frontě známo, že vyžaduje izolaci, možná proto, že vykazuje odlišné chování v různých časech.
  - Taková fronta může buď vyžadovat co nejlepší výkon za různých okolností, nebo musí být izolována tak, aby neovlivňovala negativně ostatní fronty ve fondu vyrovnávacích pamětí.

  - Každá taková fronta může být izolována do svého vlastního fondu vyrovnávacích pamětí a sady stránek.
- Chcete izolovat různé sady front od sebe navzájem z důvodů třídy služeb.
  - Každá sada front může poté 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.

Rozhodněte o nastavení pro každý fond vyrovnávacích pamětí.

Pokud používáte čtyři fondy vyrovnávacích pamětí popsané v části “Rozhodněte se o počtu fondů vyrovnávacích pamětí, které chcete definovat” na stránce 155, pak Doporučené definice pro nastavení fondu vyrovnávacích pamětí poskytují dvě sady hodnot pro velikost fondů vyrovnávacích pamětí.

První sada je vhodná pro testovací systém, druhý pro provozní systém nebo pro systém, který se nakonec stane produkčním systémem. Ve všech případech definujte fondy vyrovnávacích pamětí pomocí atributu **LOCATION**(*ABOVE*).

Tabulka 21. Doporučené definice pro nastavení fondu vyrovnávacích pamětí

Nastavení definice	Zkušební systém	Produkční systém
BUFFPOOL 0	050 vyrovnávacích pamětí	50 000 vyrovnávacích pamětí
BUFFPOOL 1	050 vyrovnávacích pamětí	20 000 vyrovnávacích pamětí
BUFFPOOL 2	050 vyrovnávacích pamětí	50 000 vyrovnávacích pamětí
BUFFPOOL 3	050 vyrovnávacích pamětí	20 000 vyrovnávacích pamětí

Potřebujete-li více než čtyři doporučené fondy vyrovnávacích pamětí, vyberte fond vyrovnávacích pamětí (1 nebo 2), který nejpřesněji popisuje očekávané chování front ve fondu vyrovnávacích pamětí a jejich velikost pomocí informací v tématu Doporučené definice pro nastavení fondu vyrovnávacích pamětí.

Ujistěte se, že je parametr MEMLIMIT nastaven dostatečně vysoko, takže všechny fondy vyrovnávacích pamětí mohou být umístěny nad pruhem.

Monitorování výkonu fondů vyrovnávacích pamětí při očekávaném načtení

Využití fondů vyrovnávacích pamětí můžete monitorovat pomocí analýzy statistik výkonu fondu vyrovnávacích pamětí. Zejména byste měli zajistit, aby fond vyrovnávacích pamětí byl dostatečně velký, aby hodnoty QPSTSOS, QPSTSTLA a QPSTDMC zůstaly na nule.

Další informace naleznete v tématu Záznamy dat správce vyrovnávací paměti.

Upravit charakteristiky fondu vyrovnávacích pamětí

Podle potřeby použijte následující body k úpravě nastavení fondu vyrovnávacích pamětí z produktu “Rozhodněte o nastavení pro každý fond vyrovnávacích pamětí.” na stránce 156.

Jako vodítko použijte statistiky výkonu z “Monitorování výkonu fondů vyrovnávacích pamětí při očekávaném načtení” na stránce 156 .

1. Provádíte-li migraci ze starší 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 pro výkon, a fondy vyrovnávacích pamětí mohou být mnohem větší, pokud jsou nad panelem.

   Avšak v každém případě byste měli mít k dispozici dostatečné skutečné úložiště, takže jsou fondy vyrovnávacích pamětí rezidentní ve skutečném úložišti. Je lepší mít menší fondy vyrovnávacích pamětí, které nemají za následek stránkování, než velké, které dělají.

Navíc neexistuje žádný bod s fondem vyrovnávacích pamětí, který je větší než celková velikost sad stránek, které ji používají, ačkoli byste měli vzít v úvahu rozšíření sady stránek, pokud k němu pravděpodobně dojde.

3. Zamířit na jednu sadu stránek na fond vyrovnávacích pamětí, protože poskytuje lepší izolaci aplikace.
4. Máte-li dostatečnou reálnou paměť, takže vaše fondy vyrovnávacích pamětí nebudou nikdy stránkovány operačním systémem, zvažte použití vyrovnávacích pamětí stránek ve svém fondu vyrovnávacích pamětí.

   To je zvláště důležité, pokud je pravděpodobné, že fond vyrovnávacích pamětí projde velkým I/O, protože šetří náklady CPU přidružené ke stránce-fixace vyrovnávacích pamětí před I/O, a stránka-unfixing them později.
5. Existuje několik výhod pro vyhledání fondů vyrovnávacích pamětí nad panelem, i když jsou dostatečně malé, aby se vešly pod sloupec. Patří mezi ně:
   - 31bitová omezení virtuálních úložišť-například více prostoru pro společné úložiště.
   - Pokud má být velikost fondu vyrovnávacích pamětí neočekávaně zvýšena, zatímco je intenzivně používána, je zde menší dopad a riziko pro správce front a jeho pracovní zátěž přidáním dalších vyrovnávacích pamětí do fondu vyrovnávacích pamětí, který je již nad panelem, než přesouvání fondu vyrovnávacích pamětí nad pruh a poté přidáním dalších vyrovnávacích pamětí.
6. Vylaďte fond vyrovnávacích pamětí nula a fond vyrovnávacích pamětí pro zprávy s krátkou životností (fond vyrovnávacích pamětí 2), takže 15% volné prahové hodnoty nebude nikdy překročeno (tedy hodnota QPSTCBSL dělená QPSTNBUF je vždy větší než 15%). Zůstane-li více než 15% vyrovnávacích pamětí volné, lze během normálního provozu do značné míry vyhnout se operacím I/O s použitím těchto fondů vyrovnávacích pamětí, ačkoli zprávy starší než dva kontrolní body jsou zapsány do sad stránek.

   Upozornění: Optimální hodnota těchto parametrů je závislá na charakteristikách jednotlivých systémů. Dané hodnoty jsou zamýšleno pouze jako vodítko a nemusí být vhodné pro váš systém.
7. SYSTEM.* fronty, které jsou velmi hluboké, například SYSTEM.CHANNEL.SYNCQmůže mít prospěch z umístění ve vlastním fondu vyrovnávacích pamětí, je-li k dispozici dostatečné úložiště.

Produkt IBM MQ SupportPac MP16 - WebSphere MQ pro z/OS Plánování kapacity & ladění poskytuje další informace o ladění fondů vyrovnávacích pamětí.

z/OS Plánování vašeho protokolovacího prostředí

Použijte toto téma k naplánování počtu, velikosti a umístění protokolů a archivaci protokolů používaných produktem IBM MQ.

Protokoly se používají pro:

- Zápis informací o obnově pro trvalé zprávy
- Zaznamenat informace o jednotkách práce pomocí trvalých zpráv
- Zaznamenat informace o změnách v objektech, jako je například definování fronty
- Záložní struktury prostředku CF

a pro další vnitřní informace.

Prostředí protokolování produktu IBM MQ je vytvořeno s použitím maker systémových parametrů pro zadání voleb, jako například: zda mají být použity jednotlivé nebo duální aktivní protokoly, jaká média mají být použita pro svazky protokolu archivace a kolik vyrovnávacích pamětí protokolu má být uloženy.

Tato makra jsou popsána v části Vytvořit zaváděcí program a datové sady protokolu a Přizpůsobte modul parametrů systému.

Poznámka: Pokud používáte skupiny sdílení front, ujistěte se, že definujete zaváděcí program a protokolové datové sady s SHAREOPTIONS (2 3).

Tento oddíl obsahuje informace o následujících tématech:

z/OS *Definice datové sady protokolu*

Toto téma vám pomůže při rozhodování o nejvhodnější konfiguraci pro datové sady protokolů.

Toto téma obsahuje informace, které vám pomohou odpovědět na následující otázky:

- Měla by vaše instalace používat jednoduché nebo duální protokolování?
- Kolik aktivních datových sad protokolů potřebujete?
- “Jak velké by měly být aktivní protokoly?” na stránce 159
- Umístění aktivního protokolu
- V 9.2.0 “Aktivní šifrování protokolu s šifrováním datové sady produktu z/OS” na stránce 160

Měla by vaše instalace používat jednoduché nebo duální protokolování?

Obecně byste měli používat duální protokolování pro produkci, abyste minimalizovali riziko ztráty dat. Chcete-li, aby váš testovací systém odrážel produkci, měli byste používat duální protokolování, jinak budou moci vaše testovací systémy používat jednoduché protokolování.

S jednoduchou protokolovací daty se zapisuje do jedné sady datových sad protokolu. S duálním protokolováním dat se zapisují do dvou sad datových sad protokolů, takže v případě problému s jednou datovou sadou protokolu, jako je například datová sada, která byla omylem odstraněna, lze použít ekvivalentní datovou sadu v jiné sadě protokolů k obnově dat.

S duálním protokolováním potřebujete dvakrát tolik DASD jako s jediným protokolováním.

Používáte-li duální protokolování, pak také používejte duální BSDS a duální archivaci, abyste zajistili adekvátní zajištění pro obnovu dat.

Duální aktivní protokolování přidá nízké náklady na výkon.

Upozornění: Použití technologií zrcadlení disku, jako je Metro Mirror, nemusí být nutně náhradou pro duální protokolování a duální sadu BSDS. Je-li zrcadlená datová sada náhodně odstraněna, obě kopie budou ztraceny.

Pokud použijete trvalé zprávy, jedno protokolování může zvýšit maximální kapacitu o 10-30% a může také zlepšit dobu odezvy.

Jednoduché protokolování používá 2-310 aktivních datových sad protokolů, zatímco duální protokolování používá 420 aktivních datových sad žurnálu k poskytnutí stejného počtu aktivních protokolů. Jednotlivý protokolování proto snižuje množství protokolovaných dat, což může být důležité v případě, že je vaše instalace omezena na I/O.

Kolik aktivních protokolových datových sad potřebujete?

Počet protokolů závisí na aktivitách správce front. Pro testovací systém s nízkou propustností by mohly být vhodné tři aktivní datové sady žurnálu. Pro systém s vysokou propustností můžete chtít maximální počet dostupných protokolů, takže pokud se vyskytne problém s odložením protokolů, budete mít více času na vyřešení problémů.

Musíte mít alespoň tři aktivní datové sady protokolů, ale je vhodnější definovat více. Je-li například čas potřebný k vyplnění protokolu pravděpodobně přiblížením času strávnému archivace protokolu během vrcholného zatížení, definujte více protokolů.

Poznámka: Sady stránek a aktivní protokolovací datové sady jsou vhodné k umístění v části přídavného adresního prostoru (EAS) a z z/OS V1.12může být také archivní soubor protokolu archivace umístěn v EAS.

Měli byste také definovat více protokolů, aby bylo možné kompenzovat možné prodlevy při archivaci protokolu. Pokud použijete archivní protokoly na pásce, umožněte čas potřebný k připojení pásky.

Zvažte dostatek aktivního protokolovacího prostoru pro uchování dat dne v den v případě, že systém nemůže archivovat kvůli nedostatku DASD, nebo protože nemůže zapisovat na pásku. Pokud se zaplní všechny aktivní protokoly, pak produkt IBM MQ nemůže zpracovat trvalé zprávy nebo transakce. Je velmi důležité mít dostatek aktivního protokolovacího prostoru.

Je možné dynamicky definovat nové aktivní datové sady protokolů jako způsob minimalizace efektu prodlev archivace nebo problémů. Nové datové sady lze rychle převést do režimu online pomocí příkazu **DEFINE LOG** , který zabrání zastavení správce front v důsledku nedostatku místa v aktivním protokolu.

Chcete-li definovat více než 31 aktivních datových sad protokolů, musíte nakonfigurovat prostředí protokolování pro použití formátu BSDS formátu verze 2. Jakmile je BSDS ve formátu verze 2 používán, lze pro každý svazek s kopií protokolu definovat až 310 aktivních datových sad žurnálu. Informace o tom, jak konvertujete na verzi BSDS formátu 2, naleznete v příručce “Plánování zvýšení maximálního adresovatelného rozsahu protokolu” na stránce 167 .

Můžete určit, zda správce front používá sadu BSDS verze 2 nebo vyšší, a to buď spuštěním obslužného programu mapy protokolu tisku (CSQJU004), nebo z zprávy CSQJ034I zadané během inicializace správce front. Konec protokolu RBA protokolu FFFFFFFFFFFFFFFF, v rámci zprávy CSQJ034I označuje, že verze 2 nebo vyšší formátu BSDS se používá. Konec rozsahu protokolu RBA produktu 0000FFFFFFFFFFFF, v rámci zprávy CSQJ034I , označuje, že je používán formát BSDS verze 1.

Když správce front používá verzi 2 nebo vyšší, formátuje BSDS, je možné použít příkaz **DEFINE LOG** k dynamickému přidání více než 31 aktivních datových sad protokolů do svazku s kopírováním protokolu.

Jak velké by měly být aktivní protokoly?

V produktu IBM MQ 8.0je maximální podporovaná velikost aktivního protokolu při archivaci na disk 4 GB. V předchozích vydáních produktu byla maximální podporovaná velikost aktivního protokolu při archivaci na disk 3 GB.

Je-li archivace na pásku, maximální velikost aktivního protokolu je 4 GB.

Měli byste vytvořit aktivní protokoly o velikosti nejméně 1 GB v produkční a testovací systémy.

Důležité: Při alokaci datových sad musíte být opatrní, protože IDCAMS provede alokaci velikosti, kterou přidělíte.

Chcete-li přidělit protokol 3 GB, uveďte jednu z následujících možností:

- Válce (4369)
- Megabajty (3071)
- STOPY (65535)
- ZÁZNAM (786420)

Každá z těchto alokuje 2.99995 GB.

Chcete-li přidělit protokol 4GB , uveďte jednu z následujících možností:

- Válce (5825)
- Megabajty (4095)
- STOPY (87375)
- ZÁZNAM (1048500)

Každá z těchto alokuje 3.9997 GB.

Při použití rozložených datových sad, kde je datová sada rozložena mezi více svazků, je uvedená hodnota velikosti alokována na každém svazku DASD, který se používá pro rozložení. Takže pokud chcete použít 4 GB protokoly a čtyři svazky pro striping, měli byste uvést:

- CYKLES (1456)
- Megabajty (1023)

Nastavení těchto atributů alokuje 4 * 1456 = 5824 Cylinderů nebo 4 * 1023 = 4092 MB.

Poznámka: Šrafování je podporováno při použití datových sad rozšířeného formátu. Toto je obvykle nastaveno správcem datových úložišť.

Informace o provádění této procedury viz Zvýšení velikosti aktivního protokolu .

Umístění aktivního protokolu

Měli byste pracovat se svým týmem pro správu úložišť a nastavit fondy úložišť pro správce front. Je třeba zvážit následující skutečnosti:

- Konvence pojmenování, takže správci front používají správné definice SMS.
- Prostor požadovaný pro aktivní a archivní protokoly. Váš fond úložišť by měl mít dostatek prostoru pro aktivní protokoly z celého dne.
- Výkon a odolnost vůči selháním.

Z výkonnostních důvodů byste měli zvážit rozložení vašich datových sad aktivního protokolu. 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 dat naleznete v předchozím textu.

Měli byste přezkoumat statistiku I/O pomocí sestav z RMF nebo podobného produktu. Proveďte revizi těchto statistik měsíčně (nebo častěji) pro datové sady produktu IBM MQ , abyste se ujistili, že nedošlo k prodlevám v důsledku umístění datových sad.

V některých situacích může být k dispozici mnoho operací I/O sady stránek prostoru IBM MQ a to může mít dopad na výkon protokolu produktu IBM MQ , pokud se nacházejí ve stejné DASD.

Používáte-li duální protokolování, ujistěte se, že každá sada aktivních a archivních protokolů se uchovává odděleně. Například je alokujte na oddělených subsystémech DASD nebo na jiných zařízeních.

Tím se snižuje riziko ztráty obou svazků, pokud je jeden ze svazků poškozen nebo zničen. Dojde-li ke ztrátě obou kopií protokolu, je pravděpodobnost ztráty dat vysoká.

Když vytváříte nová aktivní data protokolu, měli byste ji předformátovat pomocí CSQJUFMT. Není-li protokol předformátovaný, správce front formátuje protokol při prvním použití, což má vliv na výkon.

Se starší DASD s velkými spřahovanými disky, jste museli být opatrní, které svazky byly použity k získání nejlepšího výkonu.

S moderním zařízením DASD, kde jsou data rozložena přes mnoho disků PC, nemusíte se příliš obávat o to, které svazky se používají.

Váš správce datových úložišť by měl zkontrolovat podnikové úložiště DASD a zkontrolovat a vyřešit případné problémy s výkonem. Pro dostupnost byste mohli chtít použít jednu sadu protokolů na jednom subsystému DASD a duální protokoly na jiném subsystému DASD.

Aktivní šifrování protokolu s šifrováním datové sady produktu z/OS

V 9.2.0

Funkci šifrování datové sady produktu z/OS lze použít na aktivní datové sady žurnálu pro správce front spuštěné v produktu IBM MQ for z/OS 9.1.4 nebo pozdější.

Tyto aktivní datové sady žurnálu je třeba přidělit atributy EXTENDED a popisek klíče datové sady, který zajišťuje, že jsou data šifrována pomocí AES.

Informace naleznete v části Důvěrnost dat v produktu IBM MQ for z/OS s šifrováním datové sady. Další informace viz.

z/OS V 9.2.0 *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

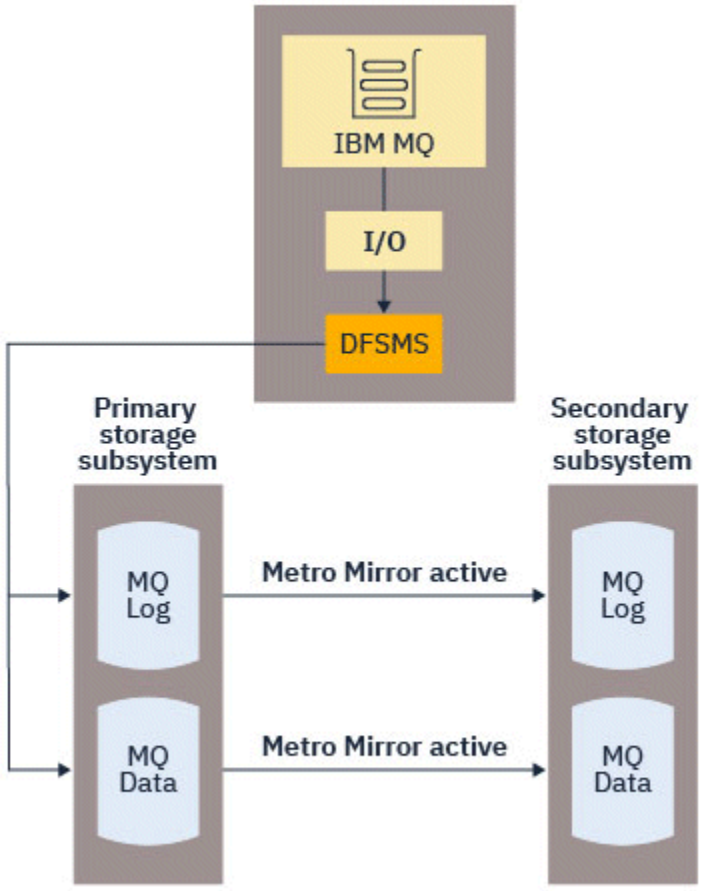
Všechny následující typy datových sad IBM MQ lze replikovat pomocí funkce Metro Mirror. Avšak přesně ty, které jsou replikovány, závisí na požadavcích na dostupnost vašeho podniku:

- 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.

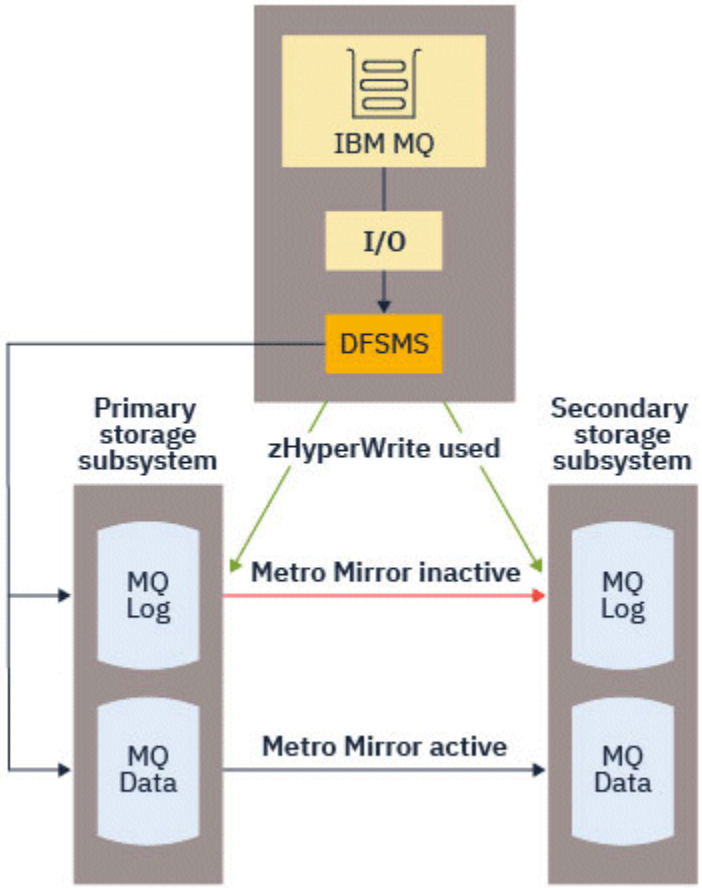


Protože oba zápisy do primárních a sekundárních úložných subsystémů musí být dokončeny před návratem zápisu do produktu IBM MQ, může mít použití funkce Metro Mirror dopad na výkon. Tento dopad na výkon musíte vyvážit s výhodami dostupnosti, které přináší funkce Metro Mirror.

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

Jsou-li splněny obě tyto podmínky, jsou pro zápis zHyperpovoleny zápisy do aktivních protokolů.

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

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.

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*

Toto téma slouží k pochopení různých způsobů údržby datových sad protokolu archivu.

Datové sady protokolu archivace můžete umístit na pásky standardního označení nebo DASD a spravovat je podle hierarchického správce úložiště dat (DFHSM). Každý logický záznam z/OS v datové sadě protokolu archivu je kontrolním intervalem VSAM z aktivní datové sady protokolu. Velikost bloku je násobkem 4 kB.

Datové sady protokolu archivace jsou dynamicky přidělovány s názvy zvolennými produktem IBM MQ. Předpona názvu datové sady, velikost bloku, název jednotky a velikosti DASD potřebné pro takové alokace jsou uvedeny v modulu parametrů systému. Můžete se také rozhodnout, že v době instalace má produkt IBM MQ přidat datum a čas do názvu datové sady protokolu archivace.

Není možné uvést s IBM MQ, určité svazky pro nové archivní protokoly, ale můžete použít rutiny správy úložiště pro správu tohoto. Pokud dojde k chybě alokace, odlehčování se odloží, dokud se nespustí další odlehčení zátěže.

Uvedete-li duální protokoly archivace v době instalace, každý řídicí interval protokolu načtený z aktivního protokolu se zapíše do dvou datových sad protokolu archivace. Záznamy protokolu obsažené ve dvojicích datových sad protokolu archivace jsou identické, ale body konce svazku nejsou synchronizovány pro vícesvazkové datové sady.

Jsou vaše archivní protokoly umístěny na pásce nebo v DASD?

Při rozhodování, zda použít pásku nebo DASD pro archivní protokoly, existuje řada faktorů, které byste měli zvážit:

- Před rozhodováním o pásce nebo disku si přečtěte své provozní procedury. Například, pokud se rozhodnete archivovat na pásku, musí být k dispozici dostatek páskové jednotky, když jsou potřeba. Po

katastrofě mohou všechny subsystémy chtít páskové jednotky a nemusíte mít tolik volných páskových jednotek, jak byste očekávali.

- Během obnovy jsou k dispozici archivní protokoly na pásce, jakmile je páska nasazena. Pokud byly použity archivy DASD a datové sady migrované na pásku pomocí hierarchického správce datových úložišť (HSM), je zde prodleva, zatímco HSM opětovně vyvolá každou datovou sadu na disk. Před použitím protokolu archivace si můžete stáhnout datové sady. Avšak není vždy možné předpovědět správné pořadí, ve kterém jsou vyžadovány.
- Když používáte protokoly archivace na DASD, je-li potřeba mnoho protokolů (což může být případ, kdy se obnovuje sada stránek po obnově ze zálohy), možná budete potřebovat značné množství DASD, aby se zadržely všechny archivní protokoly.
- V systému nebo v testovacím systému s nízkým využitím může být pohodlnější mít archivní protokoly v DASD, aby bylo eliminován nutnost připojení pásky.
- Obě vydání příkazu RECOVER CFSTRUCT a zálohování perzistentní jednotky práce vede k tomu, že žurnál je zpětně načítán. Páskové jednotky s hardwarovou kompresí provádějí na operacích, které čtou pozpátku, špatné Naplánujte dostatek protokolovaných dat v DASD, aby nedošlo k zpětnému čtení z pásky.

Archivace na DASD nabízí rychlejší obnovitelnost, ale je nákladnější než archivace na pásku. Pokud používáte duální protokolování, můžete uvést, že primární kopie protokolu archivace se bude vracet do DASD a sekundární kopie se bude nahrovat na pásku. To zvyšuje rychlost obnovy bez použití tolik DASD a můžete použít pásku jako zálohu.

Podrobné informace o tom, jak archivovat protokoly z pásky do DASD a jak provádět reverzní proces, najdete v příručce “Změna paměťového média pro archivní protokoly” na stránce 165 .

Archivace na pásku

Zvolíte-li archivaci na páskové zařízení, IBM MQ se může rozšířit na maximálně 20 svazků.

Pokud uvažujete o změně velikosti datové sady aktivního protokolu tak, aby sada odpovídala jednomu páskovému nosiči, uvědomte si, že kopie BSDS se umístí na stejný páskový nosič jako kopie aktivní datové sady žurnálu. Upravte velikost aktivní datové sady žurnálu směrem dolů a vyrovnejte prostor potřebný pro sadu BSDS na páskovém nosiči.

Pokud používáte duální protokoly archivace na pásce, je typické, že jedna kopie bude zadržena lokálně a druhá kopie bude zadržena v off-site pro použití při zotavení z havárie.

Archivace na svazky DASD

IBM MQ vyžaduje, abyste katalogizali všechny datové sady protokolu archivace přidělené na nepáskových jednotkách (DASD). Pokud se rozhodnete archivovat do DASD, parametr CATALOG makra CSQ6ARVP musí být YES. Je-li tento parametr nastaven na hodnotu NO a rozhodnete se umístit datové sady archivního protokolu do DASD, obdržíte zprávu CSQJ072E pokaždé, když je přidělena datová sada protokolu archivace, ačkoli produkt IBM MQ stále katalogizuje datovou sadu.

Pokud je datová sada protokolu archivace zadržena v DASD, datové sady protokolu archivace se mohou rozšířit na jiný svazek; je podporováno více svazků.

Pokud se rozhodnete používat DASD, ujistěte se, že alokace primárního prostoru (velikost i velikost bloku) je dostatečně velká, aby mohla obsahovat data přicházející z aktivní datové sady žurnálu nebo data z odpovídající BSDS, podle toho, která z těchto dvou hodnot je větší.

Tím je minimalizována možnost nechtěných kódů ukončení z/OS X'B37' nebo X'E37' během procesu odkládání. Přidělení primárního prostoru je nastaveno s parametrem PRIQTY (primární veličina) makra CSQ6ARVP .

V produktu IBM MQ for z/OS 8.0mohou datové sady protokolu archivu existovat ve velkých nebo v souborech sekvenčních datových sad rozšířeného formátu. Rutiny SMS ACS mohou nyní používat DSNTYPE (LARGE) nebo DSNTYPE (EXT). Tyto nebyly podporovány dříve než IBM MQ for z/OS 8.0.

Produkt IBM MQ podporuje přidělení protokolů archivace v podobě rozšířených datových sad formátu. Je-li použit rozšířený formát, maximální velikost protokolu archivace se zvýší z 65535 stop na maximální velikost aktivního protokolu 4GB. Archivní protokoly jsou vhodné pro alokaci v rozšířeném adresním prostoru (EAS) přídavných adresních svazků (EAV).

Tam, kde jsou k dispozici požadované úrovně hardwaru a softwaru, je třeba přidělit archivní protokoly do datové třídy definované pomocí příkazu COMPACTION s použitím zEDC a snížit tak diskovou paměť potřebnou k uchování protokolů archivace. Další informace viz IBM MQ for z/OS: Omezení obsazenosti úložiště pomocí produktu IBM zEnterprise Data Compression (zEDC).

Podrobnosti o úrovních hardwaru a softwaru a příklad změn profilu RACF najdete v tématu Vylepšení komprese dat zEnterprise Data Compression (zEDC) , jako například změny v profilu RACF.

Funkci šifrování datové sady produktu z/OS lze použít na archivní protokoly pro správce front spuštěné v produktu IBM MQ 8.0 nebo pozdější. Tyto archivní protokoly musí být alokovány prostřednictvím rutin automatického výběru třídy (ACS) pro datovou třídu definovanou s atributy EXTENDED a na označení klíče datové sady, který zajišťuje, že jsou data šifrována pomocí AES.

Použití SMS s datovými sadami protokolu archivu

Máte-li nainstalován subsystém správy úložišť MVS/DFP (DFSMS), můžete zapsat uživatelský výstupní filtr Automatic Class Selection (ACS) pro vaše datové sady protokolu archivace, což vám pomůže je převést do prostředí SMS.

Takový filtr může například směrovat váš výstup do datové sady DASD, kterou může spravovat DFSMS . Při použití filtru ACS tímto způsobem je třeba postupovat opatrně. Vzhledem k tomu, že server SMS vyžaduje katalogizaci datových sad DASD, je třeba zajistit, aby pole CATALOG DATA makra CSQ6ARVP obsahovalo hodnotu YES. Pokud tomu tak není, je vrácena zpráva CSQJ072E , avšak datová sada je stále katalogizována produktem IBM MQ.

Další informace o filtrech ACS najdete v tématu Datové sady, které dynamicky přiděluje DFSMShsm .

z/OS *Změna paměťového média pro archivní protokoly*

Procedura pro změnu paměťového média použitého archivační protokoly.

Informace o této úloze

Tato úloha popisuje, jak změnit paměťové médium použité pro protokoly archivace, například přesouvání z archivace na pásku do DASD.

Máte na výběr, jak provést změny:

1. Proveďte změny pouze pomocí makra CSQ6ARVP , aby byly použity od následujícího restartování správce front.
2. Proveďte změny pomocí makra CSQ6ARVP a dynamicky pomocí příkazu SET ARCHIVE . To znamená, že změny se uplatní od následujícího správce front, archivuje soubor protokolu a po restartování správce front trvale přetrvává.

Postup

1. Změna tak, aby archivní protokoly byly uloženy na DASD místo pásky:
   a) Přečtěte si oddíl “Archivace na svazky DASD” na stránce 164 a zkontrolujte parametry CSQ6ARVP .
   b) Proveďte změny následujících parametrů v souboru CSQ6ARVP
      - Aktualizujte parametr 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 uchovovaly největší část aktivního protokolu nebo BSDS.
      - Nastavte parametr CATALOG na hodnotu YES.

- Potvrďte nastavení ALCUNIT: to, co chcete. Měli byste použít BLK, protože je nezávislý na typu zařízení.
- Nastavte parametr ARCWTOR na hodnotu NO, pokud již není.

2. Změna tak, že archivní protokoly jsou uloženy na pásce místo DASD:
   a) Přečtěte si oddíl “Archivace na pásku” na stránce 164a zkontrolujte parametry CSQ6ARVP .
   b) Proveďte změny v následujících parametrech v souboru CSQ6ARVP:
      - Aktualizujte parametr UNIT a v případě potřeby parametry UNIT2 .
      - Aktualizujte parametr BLKSIZE, protože optimální nastavení pro pásku se liší od DASD.
      - Potvrďte nastavení ALCUNIT: to, co chcete. Měli byste použít BLK, protože je nezávislý na typu zařízení.
      - Zkontrolujte nastavení parametru ARCWTOR.

z/OS *Jak dlouho budu muset uchovávat protokoly archivace*

Informace v této části vám pomohou naplánovat strategii zálohování.

Způsob uchování protokolů archivu můžete uchovávat ve dnech s použitím parametru ARCRETN v příkazu USING CSQ6ARVP nebo SET SYSTEM . Po uplynutí této doby mohou být datové sady odstraněny z/OS.

Můžete ručně odstranit datové sady protokolu archivu, když již nejsou potřeba.

- Správce front může potřebovat archivní protokoly pro zotavení.

  Správce front může uchovávat pouze nejnovější 1000 archivů v BSDS, když archivní protokoly nejsou v BSDS, které nelze použít pro obnovu, a jsou určeny pouze pro účely auditu, analýzy nebo typu přehrání.
- Možná budete chtít uchovávat archivní protokoly, abyste mohli extrahovat informace z protokolů. Například extrakce zpráv z protokolu a přezkoumání toho, které ID uživatele bylo zadáno nebo získáno, zpráva.

BSDS obsahuje informace o protokolech a dalších informacích o obnově. Tato datová sada je pevnou velikostí. Když počet protokolů archivace dosáhne hodnoty MAXARCH v CSQ6LOGP, nebo když se BSDS zaplní, přepíší se nejstarší informace o protokolu archivace.

Existují obslužné programy pro odebrání položek protokolu archivace z BSDS, ale obecně jsou BSDS zalamování a překryvy nejstarším záznamem protokolu archivace.

Kdy je protokol archivace nutný

Je třeba, abyste pravidelně zazálohovali sady stránek. Frekvenci zálohování určuje, jaké archivní protokoly jsou potřebné v případě ztráty sady stránek.

Je třeba, abyste pravidelně zálohovali struktury prostředku CF. Frekvenci zálohování určuje, jaké archivní protokoly jsou potřebné v případě ztráty dat ve struktuře prostředku CF.

Protokol archivace může být potřebný pro zotavení. Následující informace vysvětlují, kdy může být potřebný protokol archivace, kde jsou problémy s různými prostředky IBM MQ .

Ztráta sady stránek

Je třeba obnovit systém ze zálohy a restartovat správce front.

Budete potřebovat protokoly od doby, kdy byla záloha provedena, stejně jako až tři datové sady protokolů před tím, než se zálohování provádí.

Všechny oblasti LPAR ztrácejí připojitelnost ke struktuře prostředku CF, nebo struktura není k dispozici.

K obnovení struktury použijte příkaz RECOVER CFSTRUCT .

Obnova struktury vyžaduje protokoly ze všech správců front, které k této struktuře přistupovaly od poslední zálohy (zpět do doby, kdy byla záloha provedena), plus samotná struktura zálohování v protokolu správce front, který zálohu vzal.

Pokud jste často zálohovali struktury prostředku CF, měla by se data nacházet v aktivních protokolech a neměli byste potřebovat archivní protokoly.

Pokud neexistuje žádná aktuální záloha struktury prostředku CF, možná budete potřebovat archivní protokoly.

Poznámka: Všechny netrvalé 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 doby zálohování

Znovusestavení struktury administrace
Potřebujete-li znovu sestavit strukturu administrace, přečtou se informace z posledního kontrolního bodu protokolu pro každého správce front v QSG.

Pokud správce front není aktivní, jiný správce front v QSG načte protokol.

Neměli byste potřebovat archivní protokoly.

Ztráta datové sady SMDS
Pokud ztratíte datovou sadu SMDS, nebo dojde k poškození datové sady, datová sada se stane nepoužitelnou a stav pro něj je nastaven na hodnotu FAILED. Struktura prostředku Coupling Facility se nezměnila.

Chcete-li obnovit datovou sadu SMDS, musíte:

1. Znovu definujte datovou sadu SMDS a
2. Proveďte zotavení struktury prostředku CF zadáním příkazu RECOVER CFSTRUCT .

   Poznámka: Všechny netrvalé zprávy ve struktuře prostředku CF budou ztraceny; budou obnoveny všechny trvalé zprávy.

Požadavek protokolů správce front je stejný jako pro zotavení ze struktury, která je nedostupná.

z/OS *Plánování zvýšení maximálního adresovatelného rozsahu protokolu*

Můžete zvýšit maximální adresovatelný rozsah protokolu nakonfigurováním správce front tak, aby používal větší adresu RBA (Relative Byte Address) protokolu.

Velikost protokolu RBA se zvětšila z IBM MQ for z/OS 8.0. Přehled této změny najdete v tématu Větší relativní bajtová adresa protokolu.

V 9.2.0 Pokud správce front není ve skupině sdílení front, můžete jej kdykoli převést na 8bajtové hodnoty protokolu RBA. Pokud následně migrujete zpět na IBM MQ for z/OS 9.0.0, ujistěte se, že používáte **OPMODE**= (*NEWFUNC,900*), jinak se správce front nespustí.

V 9.2.5 Pokud byl správce front vytvořen v produktu IBM MQ 9.2.5 nebo později, je 8bajtový protokol RBA již ve výchozím nastavení povolen, a proto nevyžaduje převod.

Předtím, než lze všechny správce front ve skupině sdílení front převést na použití osmibajtového protokolu RBA, musí být všichni správci front ve skupině sdílení front na jedné z následujících úrovní:

- V IBM MQ for z/OS 9.0.n CD, IBM MQ for z/OS 9.1.0 LTSnebo pozdější
- V IBM MQ for z/OS 9.0.0 a byla spuštěna s **OPMODE**= (*NEWFUNC,800*) nebo **OPMODE**= (*NEWFUNC,900*)

Pak můžete každý správce front změnit tak, aby používal 8bajtové hodnoty protokolu RBA protokolu. Není nezbytně nutné měnit všechny správce front najednou.

Pokud byl správce front ve skupině sdílení front převeden na použití 8 bajtových hodnot protokolu RBA protokolu, mohou ostatní správci front ve skupině sdílení front používat žurnály převedeného správce front, i když ještě nebyly převedeny, aby používaly 8bajtové hodnoty protokolu RBA protokolu. To je užitečné například pro partnerskou obnovu.

Zrušení provedení změny

Změna nemůže být vrácena.

Jak dlouho to trvá?

Změna vyžaduje restart správce front. Zastavte správce front, spusťte obslužný program CSQJUCNV proti sadě dat bootstrap (BSDS) nebo datové sady, chcete-li vytvořit nové datové sady, přejmenujte tyto zaváděcí datové sady a restartujte správce front. Obslužný program CSQJUCNV obvykle trvá spuštění několika sekund.

Jaký dopad to má?

- Při použití 8bajtového protokolu RBA má každý zápis dat do protokolovaných datových sad další bajty. Pro pracovní zátěž tvořenou trvalými zprávami se proto jedná o malý nárůst množství dat zapsaných do protokolů.
- Data zapsaná do sady stránek nebo struktura prostředku CF (Coupling Facility) nejsou ovlivněna.

Související úlohy

Implementace větší relativní bajtové adresy protokolu

z/OS Plánování inicializátoru kanálu

Inicializátor kanálu poskytuje komunikaci mezi správci front a běží ve svém vlastním adresním prostoru.

Existují dva typy připojení:

1. Aplikační připojení ke správci front v rámci sítě. Tyto informace jsou známy jako kanály klienta.
2. Připojení správce front k připojení správce front. Tyto informace jsou známy jako kanály MCA.

Moduly listener

Program modulu listener kanálu naslouchá příchozím požadavkům na síť a spouští příslušný kanál, je-li tento kanál potřeba. Chcete-li zpracovat příchozí připojení, vyžaduje iniciátor kanálu alespoň jednu konfiguraci úlohy modulu listener produktu IBM MQ . Modulu listener může být buď modul listener TCP, nebo modul listener LU 6.2 .

Každý modul listener vyžaduje port TCP nebo název jednotky LU. IBM MQ for Multiplatforms často používá port TCP/IP 1414 (předvolba).

Všimněte si, že pro každý inicializátor kanálu můžete mít více než jeden modul listener.

Protokol TCP/IP

Inicializátor kanálu může pracovat s více než jedním zásobníkem TCP na stejném obrazu z/OS . Například, jeden zásobník TCP může být pro vnitřní připojení a další zásobník TCP pro externí připojení.

Definujete-li výstupní kanál:

1. Nastavili jste cílového hostitele a port připojení. To může být buď:
   - adresa IP, například `10.20.4.6`
   - název hostitele, například `mvs-prod.myorg.com`

   Použijete-li k určení místa určení název hostitele, produkt IBM MQ použije k vyřešení adresy IP cíle DNS (Domain Name System).
2. Pokud používáte více zásobníků TCP, můžete uvést parametr **LOCLADDR** v definici kanálu, který uvádí adresu zásobníku IP, která se má použít.

Měli byste mít v plánu mít vysoce dostupný server DNS nebo servery DNS. Pokud server DNS není k dispozici, odchozí kanály nemusí být možné spustit a nelze zpracovat pravidla ověřování kanálu, která mapují příchozí připojení pomocí názvu hostitele.

APPC a LU 6.2

Pokud používáte APPC, iniciátor kanálu potřebuje název LU a konfiguraci v APPC.

Skupiny sdílení front

Chcete-li poskytnout obraz jednoho systému a povolit příchozí požadavek na připojení produktu IBM MQ , aby mohl přejít do 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 do libovolného správce front připojeného k tomuto hardwaru.
2. Virtuální IP adresa (VIPA). Je uvedena celopodniková adresa IP a tato adresa může být směrována na kteroukoli z zásobníků TCP v prostředí sysplex. Zásobník TCP jej pak může směrovat do libovolného naslouchajícího správce front v prostředí sysplex.

Ochrana provozu produktu IBM MQ

Server IBM MQ můžete nakonfigurovat tak, aby používal TLS (nebo SSL) připojení k ochraně dat na spoji. Chcete-li použít TLS, musíte použít digitální certifikáty a svazky klíčů.

Musíte také pracovat se zaměstnanci na vzdáleném konci kanálu, abyste zajistili, že budete mít kompatibilní definice IBM MQ a kompatibilní certifikáty.

Můžete řídit, která připojení se mohou připojit k produktu IBM MQ a k ID uživatele na základě

- Adresa IP
- ID uživatele klienta
- Vzdálený správce front nebo
- Digitální certifikát (viz Záznamy ověření kanálu)

Také je možné omezit aplikace klienta tím, že zajistíte, aby dodaly platné ID uživatele a heslo (viz téma Ověření připojení).

Můžete získat práci inicializátoru kanálu a poté každý kanál nakonfigurovat tak, aby používal TLS, jeden po druhém.

Monitorování inicializátoru kanálu

K dispozici jsou příkazy MQSC, které poskytují informace o inicializátoru kanálu a kanálech:

- Příkaz DISPLAY CHINIT poskytuje informace o inicializátoru kanálu a aktivních listenerech.
- Příkaz DISPLAY CHSTATUS zobrazuje aktivitu a stav kanálu.

Inicializátor kanálu může také vytvořit záznamy SMF s informacemi o úlohách inicializátoru kanálu a o aktivitě kanálu. Další informace viz “Plánování pro data SMF inicializátoru kanálu” na stránce 170.

Inicializátor kanálu vyšle 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, může být vytvořeno mnoho zpráv. Tyto zprávy můžete potlačit buď pomocí prostředku pro zpracování zpráv produktu z/OS , nebo nastavením **EXCLMSG** pomocí příkazu SET SYSTEM .

Konfigurace definic kanálů produktu IBM MQ

Je-li k sobě připojeno mnoho správců front, může být obtížné spravovat všechny definice objektů. Použití klastrování produktu IBM MQ může toto zjednodušení zjednodušit.

Uvedete dva správce front jako úplná úložiště. Ostatní správci front potřebují jedno připojení k jednomu z úložišť a jedno připojení. Jsou-li zapotřebí připojení k jiným správcům front, správce front vytváří a spouští kanály automaticky.

Pokud plánujete mít velký počet správců front v klastru, měli byste naplánovat, aby měli správci front, kteří pracují jako vyhrazená úložiště, a nemají žádný provoz aplikací.

Další informace viz “Plánování vašich distribuovaných front a klastrů” na stránce 19.

Akce před konfigurací inicializátoru kanálu

1. Rozhodněte se, zda používáte protokol TCP/IP nebo APPC.
2. Používáte-li protokol TCP, přidělte alespoň jeden port pro prostor IBM MQ.
3. Pokud potřebujete server DNS, nakonfigurujte server tak, aby byl v případě potřeby vysoce dostupný.
4. Pokud používáte APPC, přidělte jméno LU a nakonfigurujte APPC.

Akce po konfiguraci inicializátoru kanálu před tím, než přejdete do produkce

1. Naplánujte, jaká připojení budete mít:
   a. Připojení klienta ze vzdálených aplikací.
   b. Kanály MCA pro ostatní správce front a z jiných správců front. Obvykle máte kanál pro každého vzdáleného správce front a z něj.
2. Nastavte klastrování nebo se připojte k existujícímu klastrového prostředí.
3. Zvažte, zda byste potřebovali použít více zásobníků TCP, VIPA nebo externího směrovače pro dostupnost před inicializačním kanálem kanálu.
4. Plánujete-li použití TLS:
   a. Nastavení svazku klíčů
   b. Nastavení certifikátů
5. Plánujete-li používat ověřování kanálu, postupujte takto:
   a. Rozhodněte se o kritériích pro mapování příchozích relací na jména uživatelů MCA
   b. Povolit reverzní vyhledávání DNS nastavením parametru správce front **REVDNS**
   c. Zkontrolujte zabezpečení. Například odstraňte výchozí kanály a uveďte ID uživatele pouze s potřebným oprávněním v atributu **MCAUSER** pro kanál.
6. Zachyťte evidenční a statistické záznamy SMF produkované inicializačním kanálem kanálu a jejich následné zpracování.
7. Automatizujte monitorování zpráv v protokolu úlohy.
8. V případě potřeby vylaďte své síťové prostředí, abyste zlepšili propustnost. Při použití protokolu TCP zvyšuje propustnost velkých odesílacích a přijímacích mezipamětí. Můžete vynutit, aby MQ používal specifické velikosti vyrovnávací paměti TCP pomocí příkazů:

   ```
   RECOVER QMGR(TUNE CHINTCPRBDYNSZ nnnnn)
   RECOVER QMGR(TUNE CHINTCPSBDYNSZ nnnnn)
   ```

   které nastaví SO_RCVBUF a SO_SNDBUF, pro kanály na velikost v bajtech uvedené v nnnnn.

Související pojmy

“Plánování pro správce front” na stránce 142
Při nastavování správce front by mělo být vašemu plánování umožněno růst správce front, aby správce front splňoval požadavky vašeho podniku.

z/OS Plánování pro data SMF inicializátoru kanálu

Je třeba naplánovat implementaci shromažďování dat SMF pro inicializátor kanálu.

Inicializátor kanálu vytvoří dva typy záznamu:

- Statistická data s informacemi o inicializátoru kanálu a o úlohách v něm.

- Data evidence kanálu s informacemi podobnými příkazu DISPLAY CHSTATUS .

Shromažďování statistických dat spustíte pomocí příkazu:

```
START TRACE(STAT) CLASS(4)
```

a ukončete jej s použitím příkazu:

```
STOP TRACE(STAT) CLASS(4)
```

Shromažďování účtovacích dat spustíte pomocí příkazu:

```
START TRACE(ACCTG) CLASS(4)
```

a ukončete jej s použitím příkazu:

```
STOP TRACE(ACCTG) CLASS(4)
```

Můžete řídit, které kanály mají data evidence shromážděná pro použití atributu **STATCHL** v definici kanálu nebo ve správci front.

- V případě klientských kanálů je třeba nastavit produkt **STATCHL** na úrovni správce front.
- Pro automaticky definované odesílací kanály klastru můžete řídit shromažďování dat evidence pomocí atributu správce front produktu **STATACLS** .

Výchozí hodnota **STATCHL** pro správce front je 0FF. Chcete-li shromažďovat data evidence kanálu, je třeba kromě počáteční evidence trasování třídy 4 změnit hodnotu proměnné **STATCHL** z výchozí hodnoty na definici správce front nebo kanálu.

Záznamy SMF se vytvářejí, když:

- LTS Od IBM MQ for z/OS 9.2.0 do 9.2.3, time interval označený parametrem CSQ6SYSP **STATIME** uplynul, nebo **STATIME** je nula na všesměrového vysílání shromažďování dat SMF. Požadavky na shromažďování dat SMF pro inicializátor kanálu a správce front jsou synchronizovány.
- V 9.2.4 Od IBM MQ for z/OS 9.2.4 uplynul časový interval indikovaný parametry CSQ6SYSP **STATIME** nebo **ACCTIME** ; nebo, pokud je **STATIME** nebo **ACCTIME** nula v vysílání shromažďování dat SMF. 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
- Inicializátor kanálu je vypnutý. V tomto okamžiku jsou veškerá data SMF zapsána.

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, vytvoří se dvě sady dat evidence kanálu.

Statistické údaje se obvykle zapadá do jednoho záznamu SMF, ale může být vytvořeno více záznamů SMF, pokud se používá velký počet úloh.

Účtovací data se shromažďují pro každý kanál, pro který je povolen, a normálně zapadá do jednoho záznamu SMF. Je-li však aktivní velký počet kanálů, může být vytvořeno více záznamů SMF.

Náklady na shromažďování dat SMF inicializátoru kanálu jsou malé. Typicky je nárůst využití procesoru pod několika procenty a často v rámci chyby měření.

Před použitím této funkce musíte pracovat se svými systémovými programátory produktu z/OS , abyste se ujistili, že SMF má kapacitu pro další záznamy, a že změní své procesy pro extrakci záznamů SMF, aby zahrnovaly nová data SMF.

Pro data statistiky inicializátoru kanálu je typ záznamu SMF 115 a podtyp 231.

V případě dat evidence inicializátoru kanálu je typ záznamu SMF 116 a podtyp 10.

Můžete napsat své vlastní programy pro zpracování těchto dat nebo použít program SupportPac MP1B , který obsahuje program, MQSMF, pro tisk dat a pro vytváření dat ve formátu CSV (Comma Separated Values) vhodné pro import do tabulky rozložení.

Pokud dochází k problémům se zachytáváním dat SMF iniciátoru kanálu, přečtěte si další informace v tématu Řešení problémů při zachytávání dat SMF pro inicializátor kanálu (CHINIT) .

Související úlohy

Interpretace statistiky výkonu produktu IBM MQ

Odstraňování problémů s daty evidence kanálu

z/OS Plánování prostředí z/OS TCP/IP

Chcete-li dosáhnout nejlepší průchodnosti vaší sítě, musíte použít odesílací a přijímací vyrovnávací paměti TCP/IP s velikostí 64 KB nebo větší. Při použití této velikosti systém optimalizuje velikost vyrovnávací paměti.

Informace naleznete v části Co je dynamické správné nastavení 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 jsou vaše velikosti vyrovnávací paměti menší než 65536, musíte pracovat se svým síťovým týmem, abyste zvýšili hodnoty **TCPSENDBFRSIZE** a **TCPRCVBUFRSIZE** v `PROFILE DDName` v proceduře TCPIP. Můžete například použít následující příkaz:

```
TCPCONFIG TCPSENDBFRSZE 65536 TCPRCVBUFRSIZE 65536
```

Pokud nemůžete změnit nastavení systému **TCPSENDBFRSIZE** nebo **TCPRCVBUFRSIZE** v rámci celého systému, obraťte se na středisko podpory softwaru IBM .

z/OS Plánování skupiny sdílení front (QSG)

Nejjednodušším způsobem implementace prostředí sdílených front je konfigurovat správce front, přidat tohoto správce front do skupiny QSG a poté přidat další správce front do skupiny QSG.

Skupina sdílení front používá tabulky produktu Db2 k ukládání informací o konfiguraci. Existuje jedna sada tabulek používaných všemi QSGs, které sdílejí stejnou skupinu sdílení dat Db2 .

Zprávy sdílené fronty jsou uloženy ve struktuře v prostředku CF (coupling facility). Každý QSG má svou vlastní sadu struktur CF. Je třeba nakonfigurovat struktury tak, aby splňovaly vaše potřeby.

Zprávy lze rovněž ukládat do sady SMDS (Shared Message Data Sets). Velikost zprávy starší než 63KB nemůže být uložena v prostředku CF. Chcete-li tyto zprávy ukládat ve sdílených frontách, je třeba použít SMDS.

Profily zpráv a plánování kapacity

Měli byste rozumět profilu zpráv ve sdílené frontě zpráv. Níže jsou uvedeny příklady faktorů, které je třeba zvážit:

- Průměrná a maximální velikost zprávy
- Typická hloubka fronty a hloubka fronty výjimek. Například může být třeba mít dostatek kapacity pro zadržení zpráv po celý den a typická hloubka fronty je pod 100 zpráv.

Pokud se změní profil zprávy, můžete zvýšit velikost struktur nebo implementovat SMDS později.

Pokud chcete pracovat s velkým maximálním objemem zpráv, můžete produkt IBM MQ nakonfigurovat tak, aby při použití struktury dosáhl prahové hodnoty určené uživatelem pro odlehčování zpráv SMDS.

Musíte se rozhodnout, zda chcete duplexní struktury prostředku CF duplex. To je řízeno definicí struktury prostředku CF v zásadě CFRM:

1. Duplexní struktura používá dvě propojovací zařízení. Pokud se vyskytl problém s jedním prostředkem CF, není k dispozici žádné přerušení služby a struktura může být znovu sestavena na třetím prostředku CF, pokud je k dispozici. Duplexní struktury mohou mít výrazný dopad na výkon operací ve sdílených frontách.
2. Pokud struktura není duplexní, pak problém s prostředkem CF znamená, že sdílené fronty v rámci struktur v daném prostředku CF budou nedostupné, dokud nebude možné strukturu znovu sestavit v jiném prostředku CF.

   Produkt IBM MQ lze v tomto případě nakonfigurovat tak, aby v tomto případě automaticky přestavění struktury v jiném prostředku CF. Trvalé zprávy budou obnoveny z protokolů správců front.

Všimněte si, že je snadné změnit definice prostředku CF.

Strukturu můžete definovat tak, aby mohla obsahovat pouze přechodné zprávy, nebo aby mohla obsahovat trvalé a přechodné zprávy.

Struktury, které mohou uchovávat trvalé zprávy, musí být pravidelně zálohovány. Zazálohujte struktury prostředku CF minimálně každou hodinu, abyste minimalizovali čas potřebný k obnově struktury v případě selhání. Záloha se uloží do datové sady protokolu správce front, který provádí zálohování.

Pokud očekáváte vysokou propustnost zpráv ve vašich sdílených frontách, doporučuje se mít vyhrazeného správce front pro zálohování struktur prostředku CF. To zkracuje dobu potřebnou k obnově struktur, protože je třeba číst méně dat z protokolů správce front.

Kanály

Chcete-li pro aplikace připojené k objektu QSG produktu IBM MQ poskytnout jediný obraz systému pro aplikace, můžete definovat sdílené vstupní kanály. Jsou-li tyto nastaveny, může připojení přicházející do prostředí skupiny sdílení front přejít do libovolného správce front v rámci skupiny sdílení front.

Pro tyto kanály může být třeba nastavit síťový směrovač nebo virtuální adresu IP (VIPA).

Můžete definovat sdílené výstupní kanály. Instance sdíleného výstupního kanálu může být spuštěna z libovolného správce front v rámci skupiny sdílení front.

Další informace naleznete v tématu Sdílené kanály .

Zabezpečení

Prostředky produktu IBM MQ jsou chráněny pomocí externího správce zabezpečení. Pokud používáte produkt RACF, profily produktu RACF mají předponu s názvem správce front. Například fronta s názvem APPLICATION.INPUT by byl chráněn pomocí profilu ve třídě MQQUEUE s názvem `qmgrName.APPLICATION.INPUT.`

Při použití skupiny sdílení front můžete pokračovat v ochraně prostředků s profily s předponou názvu správce front nebo můžete předřadit profily s názvem skupiny sdílení front. Například `qsgName.APPLICATION.INPUT`.

Měli byste se zaměřit na použití předpony profilů s názvem skupiny sdílení front, protože to znamená, že existuje jediná definice pro všechny správce front, uložení práce a zabránění neshodě v definicích mezi správci front.

Související pojmy

“Plánování pro správce front” na stránce 142
Při nastavování správce front by mělo být vašemu plánování umožněno růst správce front, aby správce front splňoval požadavky 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

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
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

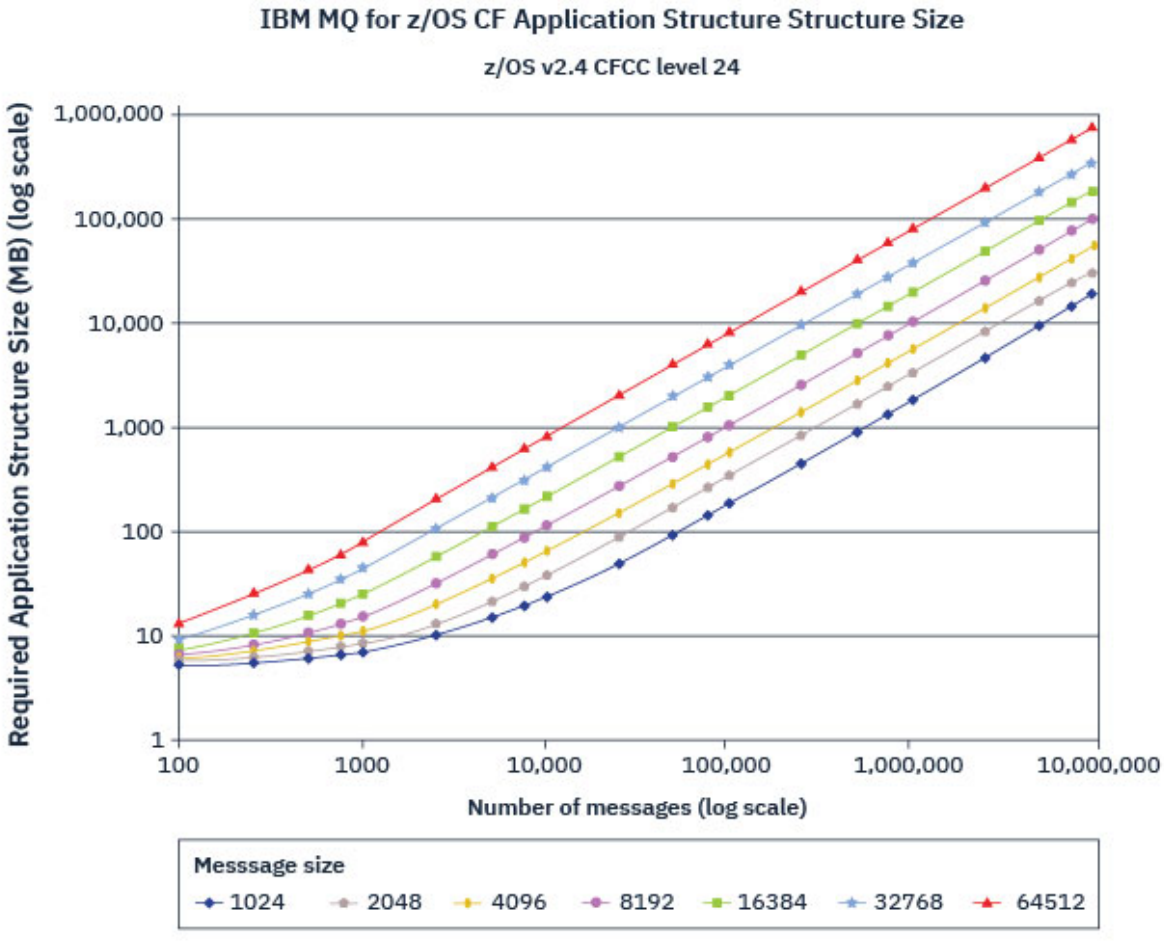
Velikost struktur aplikace požadovaných pro uchování zpráv produktu IBM MQ závisí na pravděpodobném počtu a velikosti zpráv, které mají být souběžně zadrženy ve struktuře.

Graf v souboru Obrázek 42 na stránce 177 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 se sdílenou datovou sadou zpráv (SMDS)*

Používáte-li skupiny sdílení front se odlehčování SMDS, produkt IBM MQ se musí připojit ke skupině sdílených datových sad zpráv. Toto téma vám pomůže porozumět požadavkům na datovou sadu a konfiguraci potřebnou k uložení dat zprávy produktu IBM MQ .

Datová sada sdílené zprávy (popsaná klíčovým slovem SMDS) je datová sada, kterou používá správce front k ukládání dat odlehčovaných zpráv pro sdílené zprávy uložené ve struktuře prostředku Coupling Facility.

Poznámka: Při definování datových sad SMDS pro strukturu musíte mít jednoho pro každého správce front.

Je-li tato forma odlehčování dat povolena, vyžaduje **CFSTRUCT** přidruženou skupinu sdílených datových sad zpráv, jednu datovou sadu pro každého správce front v rámci skupiny sdílení front. Skupina datových sad sdílených zpráv je definována pro IBM MQ pomocí parametru **DSGROUP** v definici **CFSTRUCT** . Další parametry lze použít k zadání dalších volitelných informací, jako je například počet vyrovnávacích pamětí, které mají být použity, 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 mohou číst všechny datové sady ve skupině.

Seznam popisující stav a atributy pro každou datovou sadu přidruženou ke struktuře se interně udržuje jako součást definice **CFSTRUCT** , takže každý správce front může zkontrolovat definici, aby zjistila, které datové sady jsou v současné době k dispozici.

Tyto informace o datové sadě lze zobrazit pomocí příkazu **DISPLAY CFSTATUS TYPE(SMDS)** za účelem zobrazení aktuálního stavu a dostupnosti, a příkaz **DISPLAY SMDS** pro zobrazení nastavení parametrů pro datové sady přidružené k zadanému **CFSTRUCT**.

Jednotlivé sdílené datové sady zpráv jsou efektivně identifikovány kombinací názvu správce front, který je vlastníkem (obvykle zadán pomocí klíčového slova **SMDS**) a názvu struktury **CFSTRUCT** .

Tento oddíl popisuje následující témata:

- Parametr DSGROUP
- Parametr DSBLOCK
- Charakteristiky sdílené datové sady zpráv
- Správa prostoru sdílené datové sady zpráv
- Přístup k datovým sadám sdílených zpráv
- Vytvoření datové sady sdílených zpráv
- Výkon datové sady sdílených zpráv a aspekty kapacity
- Aktivace datové sady sdílených zpráv

Podrobné informace o těchto parametrech najdete v tématu DEFINE CFSTRUCT .

Informace o správě vašich sdílených datových sad zpráv najdete v tématu Správa sdílených datových sad zpráv pro další podrobnosti.

Parametr DSGROUP

Parametr **DSGROUP** v definici **CFSTRUCT** určuje skupinu datových sad, do kterých mají být ukládány velké zprávy pro danou strukturu. Další parametry lze použít k určení velikosti logického bloku, který má být použit pro účely přidělení prostoru a hodnoty pro velikost fondu vyrovnávacích pamětí a volby rozšíření automatické datové sady.

Parametr **DSGROUP** musí být nastaven před vypnutým přesunutým do datových sad.

- Je-li v **CFLEVEL(5)** definován nový **CFSTRUCT** a je zadána nebo předpokládána volba **OFFLOAD(SMDS)** , pak musí být parametr **DSGROUP** zadán ve stejném příkazu.
- Pokud se stávající **CFSTRUCT** mění za účelem zvýšení hodnoty **CFLEVEL** na **CFLEVEL(5)** a je-li zadána nebo předpokládána volba **OFFLOAD(SMDS)** , pak musí být parametr **DSGROUP** zadán ve stejném příkazu, pokud již není nastaven.

Parametr DSBLOCK

Prostor v rámci každé datové sady je alokován pro fronty jako logické bloky pevné velikosti (obvykle 256 kB) pomocí parametru **DSBLOCK** v definici **CFSTRUCT** , poté přidělené jednotlivým zprávám jako rozsahy stránek o velikosti 4 kB (což odpovídá velikosti fyzického bloku a velikosti řídicího intervalu) v rámci každého logického bloku. Velikost logického bloku také určuje maximální množství dat zpráv, které lze číst nebo zapisovat do jedné operace I/O, což je stejné jako velikost vyrovnávací paměti pro fond vyrovnávacích pamětí SMDS.

Větší hodnota parametru **DSBLOCK** může zlepšit výkonnost pro velmi velké zprávy snížením počtu samostatných I/O operací. Avšak menší hodnota snižuje velikost vyrovnávací paměti požadované pro každý aktivní požadavek. Výchozí hodnota parametru **DSBLOCK** je 256 kB, což poskytuje rozumnou rovnováhu mezi těmito požadavky, takže tento parametr nemusí být normálně nutný.

Charakteristiky sdílené datové sady zpráv

Datová sada sdílené zprávy je definována jako lineární datová sada VSAM (LDS). Každá odložená zpráva je uložena v jednom nebo více blocích v datové sadě. Uložená data jsou adresována přímo podle informací v položkách prostředku Coupling Facility, jako je rozšířená forma virtuálního úložiště. K dispozici nejsou žádné samostatné indexy nebo podobné řídicí informace uložené v samotné datové sadě.

Režim přímého adresování znamená, že pro zprávy, které se vejdou do jednoho bloku, je zapotřebí pouze jedna operace I/O pro čtení nebo zápis bloku. Pokud zpráva obsahuje více než jeden blok, operace I/O pro každý blok mohou být plně překryty, aby se minimalizovala uplynulá doba, za předpokladu, že jsou k dispozici dostatečné vyrovnávací paměti.

Datová sada sdílené zprávy také obsahuje malé množství obecných informací o řízení, skládající se z hlavičky na první stránce, která zahrnuje informace o stavu zotavení a restartování, a oblast kontrolního bodu prostorové mapy, která se používá k uložení volné mapy prostoru bloků při normálním ukončení správce front.

Správa prostoru sdílené datové sady zpráv

Jako základní informace o kapacitě, výkonu a provozních aspektech může být užitečné porozumět konceptům, jak prostor ve sdílených datových sadách zpráv spravuje správci front.

Volný prostor v každé sdílené datové sadě zpráv je sledován vlastním správcem front, který vlastní správce front, pomocí prostorové mapy, která označuje počet stránek používaných v rámci každého logického bloku. Mapa prostoru se udržuje v hlavní paměti, zatímco datová sada je otevřená a uložena v datové sadě, když je normálně uzavřena. (V případě situací zotavení se mapa prostoru automaticky znovu sestaví skenováním zpráv ve struktuře prostředku Coupling Facility pro zjištění, které stránky datové sady se aktuálně používají).

Při zápisu sdílené zprávy s odloženými daty zpráv správce front alokuje rozsah stránek pro každý blok zpráv. Je-li pro určenou frontu částečně použit aktuální logický blok, přidělí správce front místo, které začíná na další volné stránce v daném bloku, jinak alokuje 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 zpráv. To se opakuje, dokud není prostor přidělen pro celou zprávu. Jakýkoli nevyužitý prostor v posledním logickém bloku se uloží jako nový aktuální logický blok pro frontu. Je-li datová sada normálně uzavřena, všechny nepoužívané stránky v aktuálních logických blocích se vrátí zpět do mapy prostoru před uložením.

Pokud byla načtena sdílená zpráva s daty odlehčenými zprávami a je připravena k odstranění, správce front zpracuje požadavek na odstranění tím, že převede položku prostředku Coupling Facility pro tuto zprávu na seznam vyčištění monitorovaný vlastnícím správcem front (což může být stejný správce front). Když záznamy dorazí do tohoto seznamu, vlastnící správce front přečte a odstraní záznamy a vrátí uvolněný rozsah stránek do mapy prostoru. Po uvolnění všech použitých stránek v logickém bloku se blok stane dostupným pro opětovné použití.

Přístup k datovým sadám sdílených zpráv

Každá datová sada sdílených zpráv musí být ve sdíleném prostoru pro přímý přístup, který je přístupný pro všechny správce front v rámci skupiny sdílení front.

Během normálního spuštění otevře každý správce front svou vlastní sdílenou datovou sadu pro přístup pro čtení a zápis a otevře všechny aktivní sdílené datové sady zpráv pro ostatní správce front pro přístup jen pro čtení, takže si mohou přečíst zprávy uložené těmito správci front. To znamená, že každé ID uživatele správce front vyžaduje alespoň přístup UPDATE k vlastní sdílené datové sadě zpráv a přístup READ ke všem ostatním datovým sadám sdílených zpráv pro danou strukturu.

Je-li nutné obnovit sdílené datové sady zpráv pomocí produktu **RECOVER CFSTRUCT**, může být proces zotavení proveden z libovolného správce front ve skupině sdílení front. Správce front, který může být použit k provedení zpracování zotavení, vyžaduje přístup UPDATE ke všem datovým sadám, které může potřebovat obnovit.

Vytvoření sdílené datové sady zpráv

Každá sdílená datová sada zpráv by měla být obvykle vytvořena dříve, než bude vytvořena nebo změněna odpovídající definice **CFSTRUCT** , aby bylo možné použít tuto formu odlehčování zpráv, protože změny definice **CFSTRUCT** se obvykle projeví okamžitě a datová sada bude nezbytná, jakmile se správce front pokusí o přístup ke sdílené frontě, která byla přiřazena této struktuře. Ukázková úloha pro přidělení a předformátování sdílené datové sady zpráv je poskytována v SCSQPROC (CSQ4SMDS). Úloha musí být přizpůsobena a spuštěna za účelem přidělení datové sady sdílené zprávy pro každého správce front, který používá CFSTRUCT s OFFLOAD (SMDS).

Pokud správce front zjistí, že podpora odlehčování byla povolena a pokusí se otevřít sdílenou datovou sadu zpráv, ale dosud nebyla vytvořena, bude datová sada sdílených zpráv označena příznakem jako

nedostupná. Správce front nebude poté moci uložit žádné velké zprávy, dokud nebude datová sada vytvořena a správce front se o tom pokusí znovu zkusit, například pomocí příkazu **START SMDSCONN** .

Datová sada sdílené zprávy je vytvořena jako lineární datová sada VSAM pomocí příkazu Access Method Services **DEFINE CLUSTER** . Definice musí určovat **SHAREOPTIONS(2 3)** , aby umožnila jednomu správci front otevřít jej pro přístup pro zápis a libovolným počtem správců front, aby jej mohli číst současně. Musí být použita výchozí velikost řídicího intervalu 4 kB. Pokud se datová sada může chtít rozšířit nad 4 GB, musí být definována pomocí datové třídy SMS, která má rozšířený atribut adresovatelnosti VSAM. Sdílená datová sada zpráv je způsobilá k umístění v části přídavného adresního prostoru (EAS).

Každá sdílená datová sada zpráv může být buď prázdná, nebo předběžně naformátována na binární nuly (pomocí obslužného programu **CSQJUFMT** nebo podobného obslužného programu, jako např. ukázková úloha SCSQPROC (CSQ4SMDS)), před jejím počátečním použitím. Je-li prázdný nebo pouze částečně zformátovaný, když se otevře, správce front automaticky formátuje zbývající prostor na binární nuly.

Informace o výkonu a kapacitě sdílené datové sady zpráv

Každá sdílená datová sada zpráv se používá k ukládání odložených dat pro sdílené zprávy zapsané do přidruženého **CFSTRUCT** správcem front, který je vlastníkem, z regionů v rámci stejného systému. Uložená data pro každou zprávu obsahují deskriptor (v současné době asi 350 bajtů), záhlaví zpráv a tělo zprávy. Každá odložená zpráva je uložena na jedné nebo více stránkách (fyzické bloky o velikosti 4 kB) v datové sadě.

Místo datové sady vyžadované pro daný počet odložených zpráv lze proto odhadnout zaokrouhlením celkové velikosti zprávy (včetně deskriptoru) na následující násobek velikosti 4 kB a poté vynásobením počtem zpráv.

Co se týče sady stránek, je-li sdílená datová sada zpráv téměř plná, může být volitelně automaticky rozbalena. Výchozí chování pro tuto automatickou expanzi lze nastavit pomocí parametru **DSEXPAND** v definici **CFSTRUCT** . Toto nastavení lze u jednotlivých správců front přepsat pomocí parametru **DSEXPAND** u příkazu **ALTER SMDS** . Automatické rozšíření se spustí, když se datová sada dosáhne o 90% plného a více prostoru je požadováno. Je-li rozšíření povoleno, ale pokus o rozšíření byl odmítnut modulem VSAM, protože při definování datové sady nebyla zadána žádná alokace sekundárního prostoru, bude zopakován pokus o rozbalení s použitím sekundárního přidělení 20% aktuální velikosti datové sady.

Je-li datová sada sdílených zpráv definována s atributem extended addressability, je maximální velikost omezena pouze na maximum 16 TB nebo 59 svazků. Tato hodnota je výrazně větší než maximální velikost 64 GB pro lokální sadu stránek.

Aktivace datové sady sdílených zpráv

Když se správce front úspěšně připojil ke struktuře prostředku Coupling Coupling Facility, zkontroluje, zda tato definice struktury určuje odlehčování pomocí přidruženého parametru **DSGROUP** . Je-li tomu tak, správce front přidělí a otevře vlastní sdílenou datovou sadu zpráv pro přístup pro zápis, poté se otevře pro přístup pro čtení k existujícím sdíleným datovým sadám zpráv vlastněných jinými správci front.

Je-li poprvé otevřena sdílená datová sada zpráv (dříve než byla zaznamenána jako aktivní ve skupině sdílení front), nebude první stránka ještě obsahovat platné záhlaví. Správce front vyplní informace záhlaví za účelem identifikace skupiny sdílení front, názvu struktury a vlastnícího správce front.

Po dokončení záhlaví správce front zaregistruje novou sdílenou datovou sadu zpráv jako aktivní a vyšle událost a upozorní všechny ostatní aktivní správce front o nové datové sadě.

Pokaždé, když správce front otevře sdílenou datovou sadu zpráv, ověřuje informace záhlaví, aby bylo zajištěno, že je stále používána správná datová sada a že nebyla poškozena.

z/OS *Plánování prostředí Db2*

Pokud používáte skupiny sdílení front, je třeba produkt IBM MQ připojit k subsystému Db2 , který je členem skupiny sdílení dat. Toto téma vám pomůže pochopit požadavky produktu Db2 použité k uchování dat produktu IBM MQ .

Produkt IBM MQ potřebuje znát název skupiny sdílení dat, ke které se má připojit, a název subsystému Db2 (nebo skupiny Db2), k němuž se má připojit, aby se dosáhlo této skupiny sdílení dat. Tato jména jsou uvedena v parametru QSGDATA makra parametru systému CSQ6SYSP (popsané v části Použití CSQ6SYSP).

Ve skupině sdílení dat se používají sdílené tabulky Db2 k zadržení:

- Konfigurační informace pro skupinu sdílení front.
- Vlastnosti sdílených a skupinových objektů produktu IBM MQ .
- Volitelně data vztahující se k odsazeným zprávám produktu IBM MQ .

V 9.2.0 Produkt IBM MQ poskytuje jednu sadu ukázkových úloh pro definování nezbytných tabulkových prostorů, tabulek a indexů produktu Db2 . Tyto úlohy využívají univerzální tabulkové prostory (UTS). Dřívější verze produktu měly dvě sady úloh, jednu pro UTS a jednu pro starší typy tabulkových prostorů, které byly zamítnuty nejnovějšími verzemi produktu Db2.

V 9.2.0 IBM MQ lze stále používat se staršími typy tabulkového prostoru a to může být vhodné v případě, že již máte existující skupinu sdílení front. Pokud však vytváříte novou skupinu sdílení front, měla by používat uživatele UTS.

V 9.2.0 Db2 V12 Úroveň funkce 508 nyní poskytuje proces migrace bez přerušení pro migraci tabulkových prostorů s více tabulkovými tabulkami do univerzálních tabulkových prostorů. Tento přístup můžete použít k migraci tabulkových prostorů s více tabulkami, které používají existující skupiny sdílení front, k univerzálním tabulkovým prostorům, aniž by došlo k výpadku celé skupiny sdílení front.

Ve výchozím nastavení používá produkt Db2 ID uživatele, který spouští úlohy jako vlastník prostředků produktu Db2 . Je-li toto ID uživatele odstraněno, budou odstraněny prostředky, které jsou k ní přidruženy, a tabulka tedy bude odstraněna. Zvažte použití ID skupiny, které vlastní tabulky, spíše než ID individuálního uživatele. To můžete provést přidáním `GROUP=groupname` na kartu JOB a uvedením `SET CURRENT SQLID='groupname'` před příkazy SQL.

Produkt IBM MQ používá prostředek služby RRS Attach produktu Db2. To znamená, že můžete zadat název skupiny Db2 , ke které se chcete připojit. Výhoda připojení k názvu připojení skupiny Db2 (spíše než specifický subsystém Db2) je, že produkt IBM MQ se může připojit (nebo znovu navázat spojení) k libovolnému dostupnému subsystému Db2 na obrazu z/OS , který je členem této skupiny. Musí existovat subsystém Db2 , který je členem skupiny sdílení dat aktivní na každém obrazu produktu z/OS , kde budete spouštět subsystém IBM MQ sdílení front, a je třeba, aby byla aktivní služba RRS.

Db2 úložný prostor

U většiny instalací je velikost požadované Db2 paměti přibližně 20 nebo 30 cylindrů na zařízení 3390. Pokud však chcete vypočítat svůj požadavek na úložiště, následující tabulka obsahuje některé informace, které vám pomohou určit, kolik úložiště Db2 vyžaduje pro data produktu IBM MQ . V tabulce je popsána délka každého řádku Db2 a každý řádek je přidán do příslušné tabulky Db2 nebo z něj odstraněn. Tyto informace použijte spolu 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 použitím funkce ADD QSG obslužného programu CSQ5PQSG .	Skupina sdílení front se odebere z tabulky s použitím funkce REMOVE QSG obslužného programu CSQ5PQSG . (Všechny řádky vztahující se k této skupině sdílení front se automaticky odstraní ze všech ostatních tabulek Db2 při odstranění záznamu skupiny sdílení front.)
CSQ.ADMIN_B_QMGR	Až 3828 bajtů	Do tabulky se přidá správce front s použitím funkce ADD QMGR obslužného programu CSQ5PQSG .	Správce front je odebrán z tabulky s použitím funkce REMOVE QMGR obslužného programu CSQ5PQSG .
CSQ.ADMIN_B_STRUCTURE	1454 bajtů	První definice lokální fronty, která uvádí atribut QSGDISP (SHARED), která pojmenovává dříve neznámou strukturu v rámci skupiny sdílení front, je definována.	Poslední definice lokální fronty, která uvádí atribut QSGDISP (SHARED), která 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, který má atribut NPMSPEED (NORMAL).	Sdílený kanál, který má atribut NPMSPEED (NORMAL), se stane neaktivním.
CSQ.ADMIN_B_STRBACKUP	514 bajtů	Do seznamu CSQ.ADMIN_B_STRUCTURE . Každá položka je fiktivní položka, dokud není spuštěn příkaz BACKUP CFSTRUCT, který přepíše fiktivní položky.	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 vymazán.
CSQ.OBJ_B_QUEUE	do 3707 bajtů	• Je definována fronta s atributem QSGDISP (GROUP). • Je definována fronta s atributem QSGDISP (SHARED). • Je otevřena modelová fronta s atributem DEFTYPE (SHAREDYN).	• Je odstraněna fronta s atributem QSGDISP (GROUP). • Fronta s atributem QSGDISP (SHARED) je odstraněna. • Dynamická fronta s atributem DEFTYPE (SHAREDYN) je uzavřena s volbou DELETE.
CSQ.OBJ_B_NAMELIST	do 15127 bajtů	Seznam názvů s atributem QSGDISP (GROUP) je definován.	Seznam názvů s atributem QSGDISP (GROUP) je odstraněn.
CSQ.OBJ_B_CHANNEL	Až 14127 bajtů	Je definován kanál s atributem QSGDISP (GROUP).	Byl odstraněn kanál s atributem QSGDISP (GROUP).

Tabulka 25. Plánování požadavků na úložiště Db2 (pokračování)

Db2 název tabulky	Délka řádku	Řádek se přidá, když:	Řádek se odstraní, když:
CSQ.OBJ_B_STGCLASS	do 2865 bajtů	Je definována třída úložiště s atributem QSGDISP (GROUP).	Třída ukládání s třídou atributů QSGDISP (GROUP) je odstraněna.
CSQ.OBJ_B_PROCESS	Až 3347 bajtů	Je definován proces s atributem QSGDISP (GROUP).	Byl odstraněn proces s atributem QSGDISP (GROUP).
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	Menší než 430 bajtů	Do tabulky se přidá správce front s použitím funkce ADD QMGR obslužného programu CSQ5PQSG .	Správce front je odebrán z tabulky s použitím 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 zprávy pro velké zprávy přidané do jedné z těchto 4 tabulek pro každý objekt BLOB zprávy. Hodnota BLOBS je dlouhá až 511 kB, takže je-li velikost zprávy větší než 711 kB, bude pro tuto zprávu existovat více objektů BLOB.	

Použití velkého počtu zpráv ve sdílené frontě o velikosti větší než 63 kB může mít významný vliv na výkon systému IBM MQ . Další informace viz SupportPac MP16, Capacity Planning and Tuning for IBM MQ for z/OS, na adrese: SupportPacs for IBM MQ a další oblasti projektu.

z/OS Plánování zálohování a obnovy

Vývoj postupů zálohování a obnovy na vašem pracovišti je nezbytný k tomu, aby se předešlo nákladným a časově náročným ztrátám dat. IBM MQ poskytuje prostředky pro obnovu obou front a zpráv do jejich aktuálního stavu po selhání systému.

Toto téma obsahuje následující sekce:

Procedury obnovy

Vyvinout následující procedury pro produkt IBM MQ:

- Vytvoření bodu obnovení.
- Zálohování sad stránek.
- Probíhá zálohování struktur CF.
- Obnova sad stránek.
- Obnova z podmínek nedostatku prostoru (protokoly IBM MQ a sady stránek).
- Probíhá obnova struktur CF.

Informace o těchto tématech viz Administrace IBM MQ for z/OS .

Seznamte se s postupy používanými na vašem webu pro následující:

- Obnova ze selhání hardwaru nebo napájení.
- Obnova ze selhání komponenty z/OS .
- Obnova z přerušení lokality pomocí offline obnovy serveru.

z/OS Tipy pro zálohování a obnovu

Toto téma vám pomůže pochopit některé úlohy zálohování a obnovy.

Proces restartování správce front obnoví vaše data do konzistentního stavu tím, že použije informace o protokolu na sady stránek. Pokud jsou vaše sady stránek poškozeny nebo nedostupné, můžete problém vyřešit pomocí záložních kopií vašich sad stránek (jsou-li k dispozici všechny protokoly). Jsou-li vaše datové sady protokolu poškozeny nebo nedostupné, nemusí být možné zcela provést zotavení.

Prohlédněte si následující body:

- Pravidelně provádět záložní kopie
- Neodstraňujte archivní protokoly, které byste mohli potřebovat
- Neměňte název DDname na sadu stránek

Pravidelně provádět záložní kopie

Bod zotavení je termín používaný k popisu sady záložních kopií sad stránek IBM MQ a odpovídajících sad dat protokolů vyžadovaných pro zotavení těchto sad stránek. Tyto záložní kopie zajišťují potenciální bod restartu pro případ ztráty sady stránek (například chyby I/O sady stránek). Pokud správce front restartujete s použitím těchto záložních kopií, budou data v produktu IBM MQ konzistentní s bodem, ve kterém byly tyto kopie odebrány. Za předpokladu, že jsou k dispozici všechny protokoly z tohoto bodu, lze IBM MQ obnovit do bodu selhání.

Čím vyšší je vaše záložní kopie, tím rychleji IBM MQ může obnovit data v sadách stránek. Obnova sad stránek závisí na všech dostupných protokolových datových sadách, které jsou k dispozici.

Při plánování obnovy je třeba určit, jak často se mají uchovávat záložní kopie a kolik úplných záložních cyklů má uchovávat. Tyto hodnoty vám říkají, jak dlouho musíte uchovávat datové sady protokolů a záložní kopie sad stránek pro zotavení produktu IBM MQ .

Když se rozhodujete o tom, jak často se mají mít záložní kopie, zvažte čas potřebný k obnově sady stránek. Potřebný čas je určen následujícím způsobem:

- Množství protokolu k procházení.
- Čas, kdy má operátor připojení a odstranění páskových nosičů s archivem.
- Čas, který trvá přečtení části protokolu potřebného k obnově.
- Čas potřebný k opětovnému zpracování změněných stránek.
- Paměťové médium použité pro záložní kopie.

- Metoda použitá k vytvoření a obnovení záložních kopií.

Obecně platí, že čím častěji zálohujete záložní kopie, tím méně času zabere, ale tím více času strávíte vytvořením kopií.

Pro každého správce front byste měli vytvořit záložní kopie následujících položek:

- Datové sady protokolu archivace
- BSDS kopie vytvořené v době archivace
- Sady stránek
- Definice objektů
- Vaše struktury prostředku CF

Chcete-li snížit riziko ztráty nebo poškození záložních kopií, zvažte:

- Uložení záložních kopií na různých paměťových svazcích do původních kopií.
- Uložení záložních kopií na jiném serveru do původních kopií.
- Uskutečnění alespoň dvou kopií každé zálohy vašich sad stránek a, pokud používáte jedno protokolování nebo jednu sadu BSDS, dvě kopie vašich archivních protokolů a BSDS. Používáte-li duální protokolování nebo BSDS, vytvořte jednu kopii obou protokolů archivu nebo BSDS.

Před přesunutím produktu IBM MQ do produkčního prostředí plně otestujte a zdokumentujte své zálohovací procedury.

Zálohování vašich sad stránek

Je třeba pravidelně zálohovat sady stránek. Některé podniky zálohujete sadu stránek dvakrát denně.

Od zálohování budete potřebovat aktivní a archivní protokoly, aby bylo možné provést obnovu pomocí zálohy. Potřebujete dostatek protokolovaných dat, aby bylo možné vrátit čtyři kontrolní body, pokud byla při spuštění správce front provedena záloha.

Nástroj ADRDSSU FastReplication můžete použít k zálohování sad stránek, a to můžete provést, když je správce front aktivní. Všimněte si, že je třeba zajistit, aby ve fondu úložišť byl dostatek místa.

Zálohování definic objektů

Vytvořte záložní kopie definic objektů. K tomu použijte funkci MAKEDEF funkce COMMAND pro obslužný program (popsané v části Použití funkce COMMAND CSQUTIL).

Tuto akci byste měli provést vždy, když provedete záložní kopie datových sad správce front a zachováte aktuální verzi.

Zálohování struktur prostředku Coupling Facility

Pokud jste nastavili nějaké skupiny sdílení front, i když je nepoužíváte, musíte provést periodické zálohy struktur prostředku CF. Použijte k tomu příkaz IBM MQ BACKUP CFSTRUCT . Tento příkaz můžete použít pouze na strukturách prostředku CF, které jsou definovány pomocí atributu RECOVER (YES). Pokud se některé položky prostředku CF pro trvalé sdílené zprávy odkazují na data odsunuté zprávy uložené v datové sadě sdílených zpráv (SMDS) nebo Db2, načtou se odlehčené údaje a jsou zálohovány pomocí položek prostředku CF. Sdílené datové sady zpráv by neměly být zálohovány samostatně.

Doporučuje se, abyste při každé hodině zálohovali všechny struktury prostředku CF, a minimalizovali tak dobu potřebnou k obnově struktury prostředku CF.

Můžete provádět všechny zálohy struktury prostředku CF v jednom správci front, což má za cíl omezit zvýšení využití protokolu na jediného správce front. Případně můžete provést zálohy všech správců front v rámci skupiny sdílení front, která má výhodu rozložení pracovní zátěže v rámci skupiny sdílení front. Bez ohledu na strategii, kterou používáte, může produkt IBM MQ vyhledat zálohu a provést RECOVER CFSTRUCT ze všech správců front ve skupině sdílení front. Protokoly všech správců front v rámci skupiny sdílení front musí být přístupné pro zotavení struktury prostředku CF.

Zálohování zásad zabezpečení zpráv

Pokud používáte produkt Advanced Message Security k vytvoření zálohy zásad zabezpečení zpráv, vytvořte zálohu pomocí obslužného programu zásad zabezpečení zpráv (CSQ0UTIL) , abyste mohli spustit produkt **dspmqspl** s parametrem -export, a poté uložte definice zásad, které jsou výstupem, do příkazu EXPORT DD.

Při každém pořízení záložních kopií datových sad správce front byste měli vytvořit zálohu zásad zabezpečení zpráv a zachovat aktuální verzi.

Neodstraňujte archivní protokoly, které byste mohli potřebovat

Je možné, že produkt IBM MQ bude muset během restartu používat protokoly archivace. Musíte uchovat dostatečné archivní protokoly, aby mohl být systém plně obnoven. IBM MQ může použít archivní protokol k obnově sady stránek z obnovené záložní kopie. Pokud jste zahodli archivní protokol, produkt IBM MQ nemůže obnovit sadu stránek do jejího aktuálního stavu. Kdy a jak zahodit protokoly archivace je popsáno v tématu Vyřazování datových sad protokolu archivace.

Můžete použít příkaz `/cpf DIS USAGE TYPE(ALL)` k zobrazení protokolu RBA protokolu a pořadového čísla protokolu (LRSN), které potřebujete k obnově vašich sad stránek správce front a struktur skupiny sdílení front. Poté byste měli pomocí příkazu print log map utility (CSQJU004) tisknout informace o sadě BSDS (bootstrap data set) pro správce front a vyhledat protokoly obsahující protokol RBA protokolu.

Pro struktury prostředku CF je třeba v každém správci front ve skupině sdílení front spustit obslužný program CSQJU004 , který vyhledá protokoly obsahující LRSN. Tyto protokoly a všechny pozdější protokoly budete potřebovat k tomu, abyste mohli obnovit sady stránek a struktury.

Neměňte název DDname na sadu stránek

IBM MQ přidružuje číslo stránky 00 00 s názvem DDname CSQP0000, číslo stránky 01 s názvem DDname CSQP0001atd. až k CSQP0099. Produkt IBM MQ zapisuje záznamy protokolu o zotavení pro sadu stránek založenou na názvu DDname, ke kterému je sada stránek přidružena. Z tohoto důvodu nesmíte přesouvat sady stránek, které již byly přidruženy ke jménu PSID DDname.

z/OS Obnova sad stránek

Pomocí tohoto tématu porozumíte faktorům, které se podílejí na obnově sad stránek, a jak minimalizovat doby restartování.

Klíčovým faktorem ve strategii zotavení se týká doba, za kterou může být výpadek správce front tolerována. Celková doba výpadku může zahrnovat čas potřebný k obnovení sady stránek ze zálohy nebo pro restartování správce front po nestandardním ukončení. Faktory ovlivňující čas restartu zahrnují, jak často zálohujete vaše sady stránek a kolik dat se zapisuje do protokolu mezi kontrolními body.

Chcete-li minimalizovat dobu restartu po nestandardním ukončení, zachovejte jednotky práce tak, aby se při restartování systému používaly maximálně dva aktivní protokoly. Pokud například navrhujete aplikaci IBM MQ , vyvarujte se umisťování volání MQGET , které má dlouhý interval čekání mezi prvním voláním MQI v rámci synchronizačního bodu a bodem potvrzení, protože by to mohlo vést k dlouhé době trvání jednotky práce. Další běžná příčina dlouhých jednotek práce je dávková intervaly více než 5 minut pro inicializátor kanálu.

Příkaz DISPLAY THREAD můžete použít k zobrazení RBA jednotek práce a pomoci vyřešit staré.

Jak často musíte zálohovat sadu stránek?

Časté zálohování sady stránek je nezbytné, je-li požadována přiměřeně krátká doba obnovy. To platí i v případě, že sada stránek je velmi malá, nebo pokud je v této sadě stránek malá aktivita na frontách.

Pokud použijete trvalé zprávy v sadě stránek, frekvence zálohování by měla být v hodinách spíše než ve dnech. To je také případ sady stránek nula.

Chcete-li vypočítat přibližnou frekvenci zálohování, začněte tím, že určíte celkovou dobu obnovy cíle. Skládá se z následujících:

1. Čas potřebný k reakci na problém.
2. Čas potřebný k obnově záložní kopie sady stránek.

   Použijete-li zálohování/obnovení SnapShot , je doba potřebná k provedení této úlohy několik sekund. Další informace o příkazu SnapShotnaleznete v příručce *DFSMSdsss Storage Administration Guide*.
3. Čas, který správce front vyžaduje k restartování, včetně další doby potřebné k obnovení sady stránek.

   To záleží nejvíce na množství dat protokolu, která musí být přečtena z aktivních a archivních protokolů od doby, kdy byla tato sada stránek naposledy zálohována. Všechna tato protokolovaná data musí být čtena kromě toho, že jsou přímo přidruženy k poškozené sadě stránek.

   Poznámka: Při použití *fuzzy backup* (je-li snímek z protokolů a sad stránek, zatímco je jednotka práce aktivní), může být nutné číst až tři další kontrolní body, a to může mít za následek potřebu číst jeden nebo více dalších protokolů.

Při rozhodování o tom, jak dlouho se má povolit obnova sady stránek, jsou faktory, které je třeba zvážit,:

- Rychlost, jakou jsou data zapsána do aktivních protokolů během normálního zpracování, závisí na tom, jak zprávy dorazí do vašeho systému, a to navíc k rychlosti zpráv.

  Zprávy přijaté nebo odeslané přes kanál mají za následek více protokolování dat, než jsou 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 celkové zátěži na vašem konkrétním subsystému DASD.

  U většiny páskových jednotek je možné dosáhnout vyšší rychlosti přenosu dat u archivovaných žurnálů s velkou velikostí bloku. Je-li však pro obnovu vyžadován protokol archivace, musí být také přečtena všechna data v aktivních protokolech.

z/OS Obnova struktur CF

V tomto tématu je třeba porozumět procesu zotavení pro struktury prostředku CF.

Alespoň jeden správce front ve skupině sdílení front musí být aktivní, aby mohl být zpracován příkaz RECVER CFSTRUCT. Zotavení struktury prostředku CF není ovlivněno dobu restartu správce front, protože zotavení provádí již aktivní správce front.

Proces obnovy se skládá ze dvou logických kroků, které jsou spravovány příkazem RECOVER CFSTRUCT:

1. Nalezení a obnova zálohy.
2. Sloučení všech protokolovaných aktualizací trvalých zpráv, které jsou uloženy ve struktuře prostředku CF, z protokolů všech správců front v rámci skupiny sdílení front, které použily strukturu prostředku CF, a aplikování změn na zálohu.

Je pravděpodobné, že druhý krok bude trvat déle, protože může být třeba načíst mnoho dat protokolu. Můžete zkrátit dobu, která trvá provedení častých zálohování, nebo pokud obnovujete více struktur prostředku CF najednou, nebo obojí.

Správce front, který provádí obnovu, vyhledá příslušné zálohy ve všech protokolech ostatních správců front pomocí dat v produktu Db2 a datových sad zaváděcího programu. Správce front přehraje tyto zálohy ve správném časovém pořadí mezi skupinou sdílení front, od těsně před poslední zálohou až do bodu selhání.

Doba, kterou trvá obnova struktury prostředku CF, závisí na množství dat protokolu pro zotavení, které je třeba přehrát, což zase závisí na frekvenci zálohování. V nejhorším případě je třeba číst protokol správce front tak dlouho, jak jej bylo možné zapsat. Takže pokud například máte skupinu sdílení front obsahující šest správců front, může přehrání protokolu trvat šest hodin, než se hodina protokolu má přehrát. Obecně

to trvá méně času než to, protože čtení lze provádět hromadně, a protože různé protokoly správce front lze číst paralelně. Jako výchozí bod doporučujeme, abyste každou hodinu zálohovali struktury prostředku CF.

Všichni správci front mohou pokračovat v práci s nesdílenými frontami a frontami v jiných strukturách prostředku mezipaměti, zatímco ve struktuře prostředku CF se nezdařila. Pokud došlo k selhání struktury administrace, musí být před zadáním příkazu RECOVER CFSTRUCT alespoň jeden ze správců front v rámci skupiny sdílení front.

Zálohování struktur prostředku CF může vyžadovat značnou kapacitu zápisu do žurnálu, a může proto způsobit velkou zátěž pro správce front, který provádí zálohování. Zvolte lehce načteného správce front pro zálohování; pro zaneprázdněné systémy přidejte dalšího správce front do skupiny sdílení front a vyhraďte jej výhradně pro provádění záloh.

z/OS Dosažení konkrétních cílů obnovy

Toto téma obsahuje pokyny k tomu, jak lze dosáhnout specifických cílů obnovy nastavením frekvence zálohování.

Pokud máte specifické cíle obnovy k dosažení, například dokončení zotavení správce front a opětovné spuštění zpracování navíc k normálnímu času spuštění během *xx* sekund, můžete použít následující výpočet k odhadu frekvence 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: Níže uvedené příklady jsou určeny ke zvýraznění potřeby zálohování vašich stránek často. Výpočty předpokládají, že většina aktivit protokolu je odvozena z velkého počtu trvalých zpráv. Existují však situace, kdy objem aktivity protokolu není snadno vypočítán. Například v prostředí skupiny sdílení front může jednotka práce, v níž jsou sdílené fronty aktualizovány spolu s dalšími prostředky, vést k zápisu záznamů UOW do protokolu IBM MQ . Z tohoto důvodu může být rychlost zápisu do protokolu aplikace ve vzorci (A) přesně odvozena pouze z zjištěné rychlosti, jakou se zapisují protokoly produktu IBM MQ .

Uvažujte například o systému, ve kterém IBM MQ MQI clients generovat celkovou zátěž 100 trvalých zpráv za sekundu. V tomto případě jsou všechny zprávy generovány lokálně.

Je-li každá zpráva o délce 1 KB, množství protokolovaných dat za každou hodinu je přibližně následující:

```
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 máte 15 minut povoleno reagovat na problém a obnovit záložní kopii sady stránek, zotavení správce front a restartování musí být dokončeno do 60 minut (3600 sekund) aplikování vzorce (A). Za předpokladu, že jsou všechna požadovaná data protokolu na hodnotě RVA2-T82 DASD, která má rychlost obnovy přibližně 2.7 MB za sekundu, znamená to, že je třeba nastavit frekvenci zálohování na úrovni stránek alespoň každých:

```
3600 seconds * 2.7 MB a second / 800 MB an hour = 12.15 hours
```

Pokud váš aplikační den IBM MQ trvá přibližně 12 hodin, každý den zálohy je vhodný. Pokud však den aplikace trvá 24 hodin, dva zálohy každý den jsou vhodnější.

Jiným příkladem může být produkční systém, v němž jsou všechny zprávy pro aplikace typu požadavek-odezva (to znamená, že je přijata trvalá zpráva v přijímacím kanálu a je generována trvalá zpráva odpovědi a odeslána odesílacím kanálem).

V tomto příkladu je dosažená velikost dávky jedna, a proto existuje jedna dávka pro každou zprávu. Pokud existuje 50 požadavků na odpověď za sekundu, celková zátěž je 100 trvalých zpráv za sekundu. Je-li každá zpráva dlouhá 1 KB, množství dat protokolovaných každou hodinu je přibližně následující:

```
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 správce front a restartovat během 30 minut (1800 sekund), znovu za předpokladu, že jsou všechny požadované údaje protokolu na RVA2-T82 DASD, je nutné, aby zálohování sady stránek bylo provedeno alespoň jednou:

```
1800 seconds * 2.7 MB a second / 1500 MB an hour = 3.24 hours
```

Pravidelné přezkoumání frekvence zálohování

Monitorujte využití protokolu produktu IBM MQ v MB za hodinu. Pravidelně proveďte tuto kontrolu a v případě potřeby nastavte frekvenci zálohování na sadu stránek.

z/OS Pokyny k zálohování pro ostatní produkty

Pokud používáte produkt IBM MQ s produktem CICS nebo IMS , je třeba vzít v úvahu také důsledky pro strategii zálohování s těmito produkty. Hierarchický správce datových úložišť (DFHSM) spravuje datové úložiště a může interagovat s úložištěm používaným produktem IBM MQ.

Zálohování a obnova pomocí DFHSM

Hierarchický správce datových úložišť (DFHSM) provádí automatickou dostupnost prostoru a správu dostupnosti dat mezi úložnými zařízeními ve vašem systému. Pokud ji použijete, musíte vědět, že data přesunuje do úložiště IBM MQ a automaticky z něj.

DFHSM efektivně spravuje váš prostor DASD přesunutím datových sad, které nebyly v poslední době použity k alternativním úložišti. Také zpřístupňuje vaše data pro obnovu tím, že automaticky kopírují nové nebo změněné datové sady na pásku nebo na záložní svazky DASD. Může odstranit datové sady nebo je přesunout na jiné zařízení. Jeho operace se vyskytují denně, v určeném čase a umožňují uchovávat datovou sadu po předem určenou dobu, než ji odstraníte nebo přesunete.

Můžete také ručně provést všechny operace DFHSM. Část *Data Facility Hierarchical Storage Manager User's Guide* vysvětluje, jak používat příkazy DFHSM. Pokud použijete DFHSM s IBM MQ, všimněte si, že DFHSM provádí následující:

- Používá katalogizované datové sady.
- Pracuje na sadách stránek a protokolech.
- Podporuje datové sady VSAM.

Zotavení a CICS

Zotavení prostředků produktu CICS není ovlivněno přítomností produktu IBM MQ. Produkt CICS rozpoznává IBM MQ jako prostředek jiného typu nežCICS (nebo externí správce prostředků) a zahrnuje produkt IBM MQ jako účastníka v jakýchkoli požadavcích na koordinaci synchronizačního bodu pomocí rozhraní správce prostředků produktu CICS (RMI). Další informace o zotavení produktu CICS naleznete v příručce *CICS Recovery and Restart Guide*. Informace o rozhraní správce prostředků produktu CICS naleznete v příručce *CICS Customization Guide*.

Zotavení a IMS

Produkt IMS rozpoznává IBM MQ jako externí subsystém a jako účastníka v koordinaci synchronizačního bodu. Zotavení IMS pro prostředky externího subsystému je popsáno v příručce *IMS Customization Guide*.

z/OS Příprava na zotavení na alternativním serveru

Pokud dojde k celkové ztrátě výpočetního střediska IBM MQ , můžete se zotavit na jiném systému IBM MQ na pracovišti obnovy.

Chcete-li obnovit systém IBM MQ na pracovišti obnovy, musíte pravidelně zálohovat sady stránek a protokoly. Stejně jako u všech operací obnovení dat jsou cíle zotavení z havárie ztraceny jako malá data, zpracování pracovní zátěže (aktualizace) a čas, jak je to možné.

Na pracovišti obnovy:

- Správce front IBM MQ zotavení **musí** mít stejný název jako ztracený správce front.
- Ujistěte se, že modul parametrů systému použitý ve správci front pro zotavení obsahuje stejné parametry jako ztracený správce front.

Proces zotavení z havárie je popsán v příručce Administrace IBM MQ for z/OS.

z/OS Příklad aktivity zálohování správce front

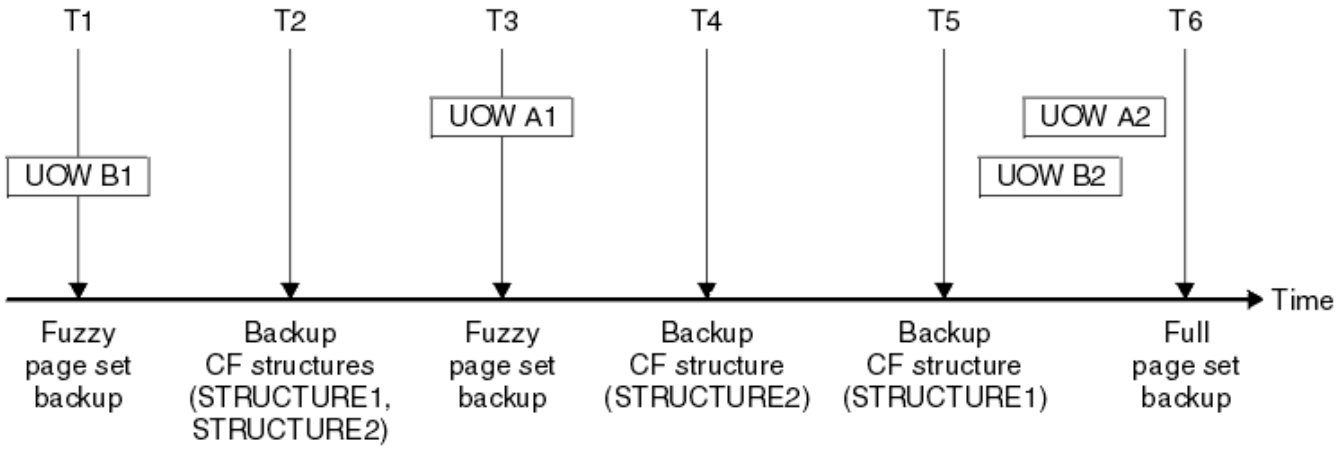
Toto téma se zobrazuje jako příklad aktivity zálohování správce front.

Při plánování strategie zálohování správce front je důležité zvážit zachování správného objemu dat protokolu. Téma Správa protokolů popisuje, jak určit, které datové sady protokolů jsou vyžadovány, podle odkazu na systémovou obnovu RBA správce front. Produkt IBM MQ určuje systémovou obnovu RBA pomocí informací o následujících tématech:

- Momentálně aktivní jednotky práce.
- Aktualizace sady stránek, které dosud nebyly vyprázdněny z fondu vyrovnávacích pamětí na disk.
- Zálohy struktury prostředku Coupling Facility a informace o tom, zda tento protokol správce front obsahuje informace potřebné pro všechny operace zotavení, které je používají.

Musíte zachovat dostatečné množství dat protokolu, abyste mohli provést obnovu médií. Zatímco obnova systému RBA se zvyšuje v čase, množství dat protokolu, která musí být uložena, se sníží pouze při provedení následných záloh. Zálohy struktury prostředku CF jsou spravovány produktem IBM MQa při vykazování obnovy RBA systému se berou v úvahu také. To znamená, že v praxi se množství dat protokolu, která musí být uchována, zmenšují, když se vezmou zálohy sady stránek.

Obrázek 43 na stránce 193 uvádí příklad aktivity zálohování na správci front, který je členem skupiny sdílení front, jak se obnova RBA liší u každé zálohy, a jak to ovlivní množství dat protokolu, která musí být uchována. 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 se děje v každém okamžiku:

Bod v čase T1
Vytvoří se fuzzy zálohování vašich sad stránek, jak je popsáno v tématu Jak zálohovat a obnovovat sady stránek.

Systémové zotavení RBA správce front je nejnižší z následujících hodnot:

- V tomto okamžiku se zálohují centrály pro obnovu sad stránek, které jsou zálohovány.
- Nejnižší hodnota RBA zotavení potřebná pro zotavení aplikačních struktur prostředku CF. Týká se obnovení záloh STRUCTURE1 a STRUCTURE2 vytvořených dříve.
- Zotavení RBA pro nejstarší aktuálně aktivní jednotku práce v rámci správce front (UOWB1).

Obnovení adresy RBA systému pro tento časový okamžik je dáno zprávami vydávané příkazem DISPLAY USAGE, který je součástí procesu fuzzy zálohování.

Bod v čase T2
Vytvoří se zálohy struktur CF. Struktura CF STRUCTURE1 je zálohována jako první, za kterou následuje STRUCTURE2.

Množství protokolovaných dat, které musí být zachovány, se nemění, protože stejná data, která jsou určena ze zotavení systému RBA na T1 , jsou stále požadována pro zotavení pomocí záloh nastavených na úrovni T1.

Bod v čase T3
Je vytvořena další fuzzy záloha.

Systémové zotavení RBA správce front je nejnižší z následujících hodnot:

- V tomto okamžiku se zálohují centrály pro obnovu sad stránek, které jsou zálohovány.
- Nejnižší hodnota RBA zotavení vyžadovaná pro zotavení struktury prostředku CF STRUCTURE1, protože STRUCTURE1 byla zálohována před STRUCTURE2.
- Obnovení adresy RBA pro nejstarší aktuálně aktivní jednotku práce v rámci správce front (UOWA1).

Obnovení adresy RBA systému pro tento časový okamžik je dáno zprávami vydávané příkazem DISPLAY USAGE, který je součástí procesu fuzzy zálohování.

Nyní můžete snížit zachovaná data protokolu, jak je určeno touto novou obnovou systému RBA.

Bod v čase T4
Bude provedena záloha struktury prostředku CF STRUCTURE2. Obnovení adresy RBA pro zotavení nejstarší vyžadované zálohy struktury prostředku CF se vztahuje k záloze struktury CF STRUCTURE1, která byla zálohována v čase T2.

Vytvoření této zálohy struktury prostředku CF nemá žádný vliv na množství dat protokolu, která musí být uchována.

Bod v čase T5
Bude provedena záloha struktury prostředku CF STRUCTURE1. Zotavení RBA pro zotavení nejstarší vyžadované zálohy struktury prostředku CF se nyní vztahuje k zotavení struktury prostředku CF STRUCTURE2, které bylo zálohováno v čase T4.

Vytvoření této zálohy struktury prostředku CF nemá žádný vliv na množství dat protokolu, která musí být zachována.

Bod v čase T6
Úplná záloha je převzata do sad stránek, jak je popsáno v tématu Jak zálohovat a obnovovat sady stránek.

Systémové zotavení RBA správce front je nejnižší z následujících hodnot:

- V tomto okamžiku se zálohují centrály pro obnovu sad stránek, které jsou zálohovány.
- Nejnižší hodnota RBA zotavení potřebná pro zotavení struktur prostředku CF. Vztahuje se k zotavení struktury prostředku CF STRUCTURE2.
- Obnovení adresy RBA pro nejstarší aktuálně aktivní jednotku práce v rámci správce front. V tomto případě nejsou k dispozici žádné aktuální jednotky práce.

Obnovení adresy RBA systému pro tento časový okamžik je dáno zprávami vydávané příkazem DISPLAY USAGE, který je součástí úplného procesu zálohování.

Opět lze snížit uchovaná data protokolu, protože obnova systému RBA, přidružená k úplné záloze, je novější.

z/OS Plánování prostředí z/OS UNIX

Určité procesy v rámci správce front produktu IBM MQ , inicializátoru kanálu a mqweb serveru používají produkt z/OS UNIX System Services (z/OS UNIX) k jejich běžnému zpracování.

ID uživatelů spuštěných úloh správce front a inicializátoru kanálu potřebují segment OMVS s definovaným identifikátorem UID, aby byl umožněn přístup k produktu z/OS UNIX. ID uživatele nevyžadují žádná speciální oprávnění v produktu z/OS UNIX.

Poznámka: Ačkoli správce front a inicializátor kanálu využívají možnosti produktu z/OS UNIX (například rozhraní se službami TCP/IP), nemusí přistupovat k žádnému z obsahu instalačního adresáře produktu IBM MQ v systému souborů z/OS UNIX . Výsledkem je, že správce front a inicializátor kanálu nevyžaduje žádnou konfiguraci k určení cesty pro systém souborů produktu z/OS UNIX .

Parametr mqweb, který je hostitelem produktů IBM MQ Console a REST API, využívá soubory v instalačním adresáři produktu IBM MQ v systému souborů z/OS UNIX . Také potřebuje přístup k jinému systému souborů, který se používá k ukládání dat, jako jsou například konfigurační soubory a soubory protokolů. Kód JCL spouštěné úlohy mqweb je třeba upravit tak, aby odkazoval na tyto systémy souborů produktu z/OS UNIX .

Obsah adresáře IBM MQ v systému souborů z/OS UNIX se také používá v aplikacích připojujících se k produktu IBM MQ. Například aplikace používající rozhraní IBM MQ classes for Java nebo IBM MQ classes for JMS .

Informace o příslušných pokynech pro konfiguraci naleznete v následujících tématech:

- Proměnné prostředí relevantní pro produkt IBM MQ classes for Java
- Knihovny produktuIBM MQ classes for Java
- Nastavení proměnných prostředí
- Konfigurace knihoven JNI (Java Native Interface)

z/OS Plánování pro databázi Advanced Message Security

TLS (nebo SSL) lze použít k šifrování a ochraně zpráv tekoucích na síti, ale to neochraňuje zprávy, když jsou ve frontě ("v klidu"). Produkt Advanced Message Security (AMS) ochraňuje zprávy od okamžiku, kdy jsou poprvé vloženy do fronty, dokud nejsou k jejich použití, takže mohou tuto zprávu číst pouze určení příjemci zprávy. Zprávy jsou šifrovány a podepsány během zpracování vkládání a nechráněné během zpracování získávání.

Produkt AMS lze nakonfigurovat tak, aby chránil zprávy různými způsoby:

1. Zprávu lze podepsat. Zpráva je v čistém textu, ale je zde kontrolní součet, který je podepsán. To umožňuje detekovat jakékoli změny v obsahu zprávy. Z podepsaného obsahu můžete identifikovat, kdo podepsal data.
2. Zprávu lze zašifrovat. Obsah není viditelný nikomu bez dešifrovacího klíče. Dešifrovací klíč je šifrován pro každého příjemce.
3. Zprávu lze zašifrovat a podepsat. Dešifrovací klíč je šifrován pro každého příjemce a od podpisu můžete identifikovat, kdo odeslal zprávu.

Šifrování a podepisování využívají digitální certifikáty a svazky klíčů.

Klienta můžete nastavit tak, aby používal AMS, takže data jsou chráněna před tím, než budou data vložena do kanálu klienta. Chráněné zprávy mohou být odeslány do vzdáleného správce front a vy potřebujete nakonfigurovat vzdáleného správce front, aby tyto zprávy zpracoval.

nastaveníAMS

Adresní prostor AMS se používá pro práci s AMS . To má další nastavení zabezpečení, pro poskytnutí přístupu k použití klíčových řetězců a certifikátů a ochranu jejich ochrany.

Fronty, které mají být chráněny pomocí obslužného programu (CSQ0UTIL), můžete nakonfigurovat tak, aby definovaly zásady zabezpečení pro fronty.

Jakmile je AMS nastaveno

Musíte nastavit digitální certifikát a svazek klíčů pro osoby, které vložila zprávy, a osoby, které získají zprávy.

Pokud uživatel, Alice, na serveru z/OS potřebuje odeslat zprávu Bobovi, potřebuje AMS kopii veřejného certifikátu pro Boba.

Pokud Bob chce zpracovat zprávu od Alice, AMS potřebuje veřejný certifikát pro Alice nebo stejný certifikát certifikační autority, který používá Alice.

Upozornění: Je třeba provést následující akce:

- Pečlivý plán, který může dát nebo dostat z fronty
- Identifikujte osoby a jejich názvy certifikátů.

Je snadné dělat chyby, a problémy mohou být těžké vyřešit.

Související pojmy

“Plánování pro správce front” na stránce 142
Při nastavování správce front by mělo být vašemu plánování umožněno růst správce front, aby správce front splňoval požadavky vašeho podniku.

z/OS Plánování pro databázi Managed File Transfer

Tento oddíl se používá jako návod, jak nastavit svůj systém ke spuštění produktu Managed File Transfer (MFT) v 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 9.2.0, například v adresáři `/mqm/V9R2M0`
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

V 9.2.0 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 9.2 Soubory PDF pro dokumentaci k produktu a Adresáře programů.

z/OS Plánování pro Managed File Transfer -topologie

Toto téma se používá jako vodítko pro topologii, kterou potřebujete ve svém systému ke spuštění produktu Managed File Transfer (MFT) v systému z/OS.

Managed File Transfer Správci front

Topologie produktu IBM MQ Managed File Transfer sestávají z následujících položek:

Agenti a jejich přidružené správci front
Agent používá systémové fronty, jejichž hostitelem je správce front agenta, aby spravoval informace o stavu a přijímal požadavky na práci.

Správce front příkazů.
Ten se chová jako brána do topologie produktu MFT . Je připojen ke správcům front agenta buď prostřednictvím odesílacích kanálů, přijímacích kanálů, nebo klastrování. Jsou-li spuštěny určité příkazy, připojí se přímo ke správci front příkazů a odešlou zprávu na uvedeného agenta. Tato zpráva je směrována přes síť IBM MQ se správcem front agenta, kde je vyzvedávána agentem a zpracována.

Koordinační správce front
Toto je centrální rozbočovač, který má znalosti o celé topologii. Koordinační správce front je připojen ke všem správcům front agenta v topologii prostřednictvím odesílacích a přijímacích kanálů nebo pomocí klastrování. Agenti pravidelně publikují informace o stavu koordinačnímu správci front a ukládají tam jejich přenosové šablony.

Jeden správce front je možné provést více rolí v rámci topologie. Jeden správce front může být například konfigurován jako koordinačního správce front i správce front příkazů pro topologii.

Používáte-li více správců front, je třeba nastavit kanály mezi správci front. To můžete provést buď pomocí klastrování, nebo pomocí dvoubodových spojení.

Při použití produktu IBM MQ Managed File Transfer for z/OSje třeba vzít v úvahu počet věcí, které je třeba vzít v úvahu při určování, které správce front mají být použity pro různé role v rámci topologie.

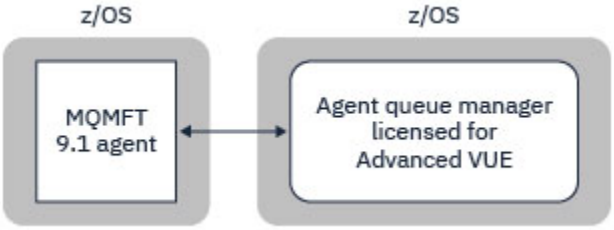
Správci front agenta

Správce front agenta pro agenta IBM MQ Managed File Transfer for z/OS musí být spuštěn na serveru z/OS.

Pokud:

- Agent spouští produkt Managed File Transfer for z/OS na serveru 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 na systému z/OS se mohou připojit ke správci front pomocí přenosu CLIENT, za předpokladu, že správce front je licencován pro rozšířenou VUE.

Pokud:

- Agent spouští produkt Managed File Transfer for z/OS na serveru IBM MQ 9.0 nebo starším
- Nebo správce front agenta spouští produkt Managed File Transfer for z/OS na serveru IBM MQ 9.0 nebo později a správce front agenta je licencován buď pro produkt MFT, IBM MQ Advanced for z/OS, nebo pro Advanced VUE .

Agent se musí připojit ke správci front pomocí přenosu BINDINGS.

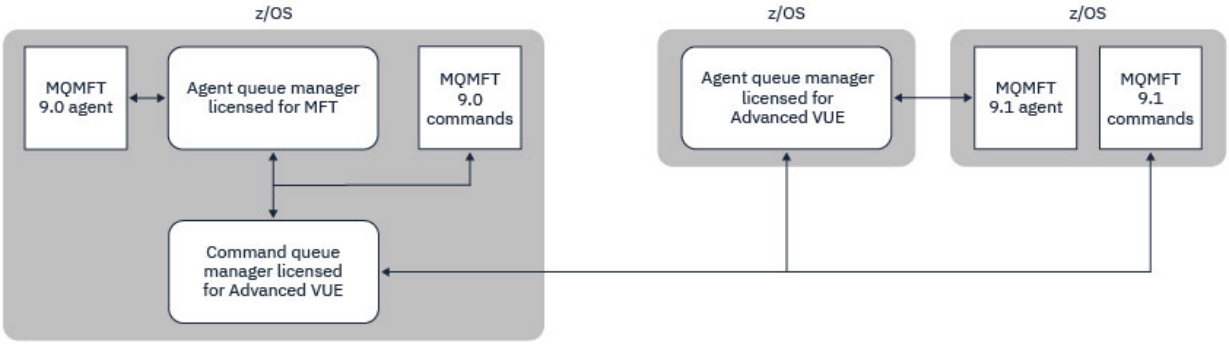
Obrázek 45. Agenti MFT 9.0 na systémech z/OS a 9.1 , kteří mají správce front agenta licencovaný buď pro MFT nebo IBM MQ Advanced, se musí připojit pomocí přenosu BINDINGS.

Správci front příkazů

Téma Které příkazy a procesy produktu MFT , které se připojují ke správci front , obsahuje všechny příkazy, které se připojují ke správci front příkazů pro topologii produktu Managed File Transfer .

Poznámka: Při spouštění těchto příkazů v systému z/OSmusí být správce front příkazů také umístěn v systému z/OS.

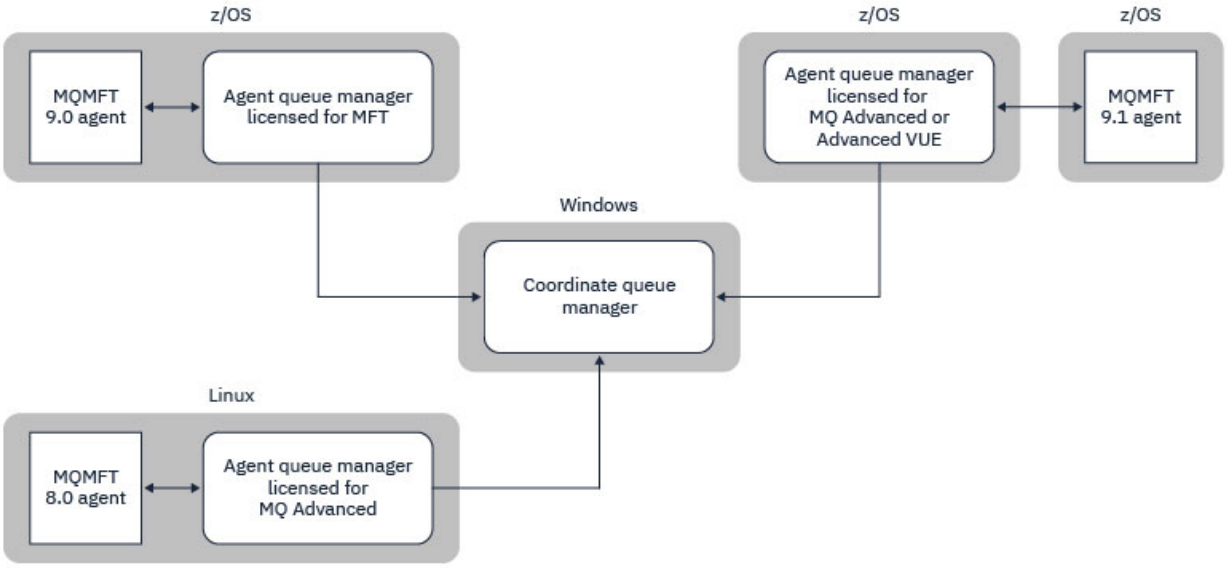
Je-li správce front příkazů licencován pro produkt Advanced VUE, mohou se příkazy připojit ke správci front pomocí přenosu CLIENT. Jinak se příkazy musí připojit ke správci front příkazů pomocí přenosu BINDINGS.



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 umístěn v systému z/OS .

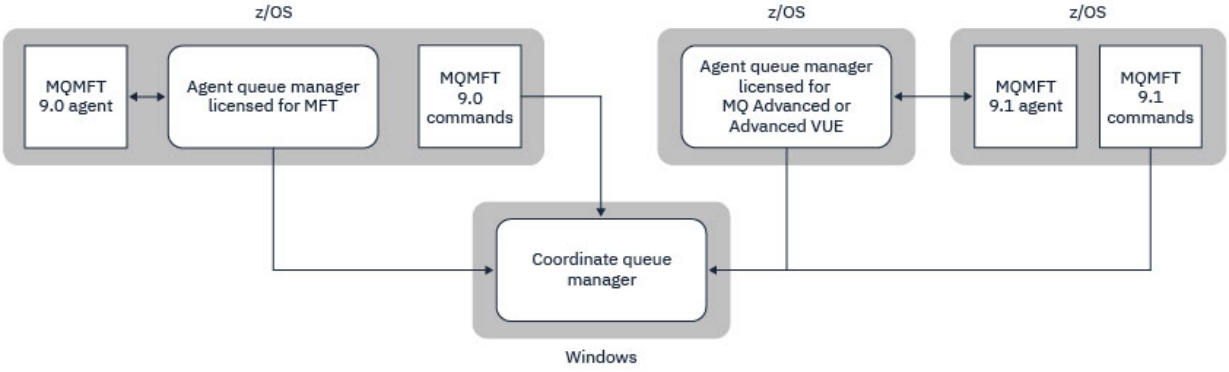
Koordinační správci front

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 je spuštěn na platformě více platforem.



Obrázek 47. Agenty MFT spuštěné v produktu z/OS mohou být součástí topologie MFT, kde je koordinační správce front spuštěn na víceplatformové platformě IBM MQ .

Téma Které příkazy a procesy produktu MFT se připojují ke správci front , obsahuje příkazy, které se připojují ke koordinačním správci front pro topologii produktu Managed File Transfer . Tyto příkazy je možné spustit v systému z/OS a poté se připojit ke koordinačnímu správci front spuštěnému na jiné platformě.



*Obrázek 48. Určité příkazy, jako například **fteListAgents**, se připojují přímo ke koordinačnímu správci front pro topologii produktu MFT .*

Kolik agentů potřebuji?

Agenti dělají práci v přenosu dat a když vytvoříte požadavek na přenos dat, uvedete název agenta.

Ve výchozím nastavení může agent zpracovávat 25 odesílat a 25 požadavků na příjem souběžně. Tyto procesy můžete nakonfigurovat. Další informace naleznete v tématu Konfigurační volbyManaged File Transfer v systému z/OS .

Pokud je agent zaneprázdněn, je práce ve frontě. Doba potřebná ke zpracování požadavku závisí na více faktorech, například na množství dat, která mají být odeslána, o šířce pásma sítě a o prodlevě v síti.

Je možné, že budete chtít pracovat paralelně s více agenty.

Můžete také řídit, ke kterým prostředkům může agent přistupovat, takže byste mohli chtít, aby někteří agenti mohli pracovat s omezenou podmnožinou dat.

Chcete-li zpracovávat požadavky s jinou prioritou, můžete pro nastavení priority úloh použít více agentů a použít správce pracovní zátěže.

Spuštění agentů

Obvykle jsou agenti přerušitelné procesy. Tyto procesy lze zadat jako úlohy, které se spouštějí dávkově, nebo jako spuštěné úlohy.

z/OS Plánování pro produkt Managed File Transfer -aspekty zabezpečení

Toto téma popisuje, jaké aspekty zabezpečení potřebujete ve svém systému ke spuštění produktu Managed File Transfer (MFT) v systému z/OS.

Zabezpečení

Musíte identifikovat, která ID uživatelů se budou používat pro konfiguraci MFT a pro operaci MFT.

Je třeba identifikovat soubory nebo fronty, které přenádíte, a která ID uživatelů budou předávat požadavky na přenos MFT.

Když přizpůsobíte agenty a registrátor, uvedete skupinu uživatelů, kteří mají povoleno spouštět služby MFT, nebo administraci MFT.

Tuto skupinu byste měli nastavit před tím, než začnete upravovat MFT. Když MFT používá fronty IBM MQ , pokud máte ve správci front povoleno zabezpečení, MFT vyžaduje 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
SYSTEM.FTE.AUTHMON1.agent_name	Aktualizovat

Pomocí uživatelského pískoviště můžete určit, které části systému souborů má uživatel, který požaduje přenos, přístup.

Chcete-li povolit uživatelský sandbox, 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 naleznete v tématu Práce s pískovišti uživatelů .

Toto ID uživatele je konfigurováno v souborech `UserSandboxes.xml` .

Tento soubor XML má informace jako ID uživatele nebo ID uživatele ID* a seznam prostředků, které lze použít (zahrnout), nebo jej nelze použít (vyloučit). Je třeba definovat specifická ID uživatelů, která mohou přistupovat k prostředkům, které jsou 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. Je-li zadán parametr `type=queue` , prostředek je buď název fronty, nebo `queue@qmgr`.
2. Pokud prostředek začíná na `//`, prostředek je datovou sadou; jinak je prostředek souborem v z/OS UNIX.
3. ID uživatele je ID uživatele z struktury MQMD, takže to nemusí odrážet ID uživatele, který tuto zprávu skutečně vkládá.
4. Pro požadavky na lokálního správce front můžete použít objekt MQADMIN CONTEXT.* omezit počet uživatelů, kteří mohou tuto hodnotu nastavit.
5. Pokud jde o požadavky přicházející ve vzdáleném správci front, musíte předpokládat, že distribuovaní správci front mají povoleno zabezpečení, aby se zabránilo neautorizovanému nastavení ID uživatele ve struktuře MQMD.
6. ID uživatele SYSPROG1 na počítači se systémem Linux je stejné ID uživatele SYSPROG1 pro kontrolu zabezpečení na systému z/OS.

z/OS Plánování použití produktů IBM MQ Console a REST API v systému 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 MQ Console umožňuje použití webového prohlížeče pro administraci správců front. Produkt REST API poskytuje jednoduché programové rozhraní pro aplikace určené k administraci správce front a pro provádění systému zpráv.

Instalační a konfigurační soubory

Je třeba nainstalovat funkci produktu IBM MQ for z/OS UNIX System Services Web Components , která nainstaluje soubory potřebné ke spuštění příkazu mqweb v produktu z/OS UNIX System Services (z/OS UNIX). Je třeba, abyste byli obeznámeni s produktem z/OS UNIX , abyste mohli nakonfigurovat a spravovat mqweb server.

Soubory produktu IBM MQ v produktu z/OS UNIX jsou nainstalovány s různými atributy, které jsou vyžadovány pro správnou činnost příkazu mqweb. Pokud potřebujete zkopírovat instalační soubory produktu IBM MQ z/OS UNIX , například pokud jste nainstalovali produkt IBM MQ na jeden systém a spouštíte produkt IBM MQ na jiném systému, měli byste zkopírovat soubor IBM MQ ZFS vytvořený

během instalace a připojit jej pouze ke čtení v místě určení. Kopírování souborů jiným způsobem může způsobit ztrátu některých atributů souboru.

Při vytváření uživatelského rozhraní mqweb je třeba se rozhodnout pro umístění a vytvořit adresář uživatelů produktu Liberty . Tento adresář obsahuje konfigurační soubory a soubory protokolů a umístění může být podobné jako `/var/mqm/mqweb`.

Použití produktů MQ Console a REST API se správci front na různých úrovních

Moduly MQ Console a REST API mohou přímo komunikovat pouze se správci front spuštěnými ve stejné verzi, vydání a úpravě (VRM). Například MQ Console a REST API dodané s IBM MQ 9.1.0 mohou interagovat pouze s lokálními správci front v IBM MQ 9.1.0, a MQ Console a REST API dodané s IBM MQ 9.0.5 může interagovat pouze s lokálními správci front na IBM MQ 9.0.5.

Pro produkt REST APImůžete pomocí konfigurace správce front brány spravovat správce front v jiné verzi z mqweb serveru. Potřebujete však alespoň jednoho správce front ve stejné verzi jako správce front brány, aby se choval jako správce front brány. Další informace viz Vzdálená administrace pomocí REST API.

Migration

Máte-li pouze jednoho správce front, můžete spustit příkaz mqweb server jako jedinou spuštěnou úlohu a změnit knihovny, které používá při migraci správce front.

Máte-li více než jeden správce front, můžete během migrace spustit příkaz mqweb servery v různých verzích pomocí spuštěných úloh s různými názvy. Tyto názvy mohou být libovolný název. Můžete například spustit server IBM MQ 9.1.0 mqweb pomocí spuštěné úlohy s názvem MQWB0910a pomocí spuštěné úlohy s názvem MQWB0905spustit příkaz IBM MQ 9.0.5 mqweb.

Po provedení migrace správců front z jedné verze na novější verzi budou správci front k dispozici v produktu mqweb pro pozdější verzi a nebudou již k dispozici na webovém serveru pro dřívější verzi.

Po provedení migrace všech správců front na novější verzi můžete odstranit parametr mqweb pro předchozí verzi.

Porty HTTP

Server mqWeb používá až dva porty pro protokol HTTP:

- Jeden pro HTTPS, s výchozí hodnotou 9443.
- Jeden pro HTTP. Protokol HTTP není ve výchozím nastavení povolen, ale je-li povolen, má výchozí hodnotu 9080.

Pokud se používají výchozí hodnoty portů, je třeba přidělit další porty. Máte-li 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 server mqweb používá, naleznete v části Konfigurace portů HTTP a HTTPS.

Chcete-li zobrazit informace o portu, můžete použít následující příkaz TSO:

```
NETSTAT TCP tcpip (PORT portNumber)
```

kde *tcpip* je název adresního prostoru protokolu TCP/IP a *portNumber* určuje číslo portu, o kterém se mají zobrazit informace.

Zabezpečení-spuštění serveru mqweb

ID uživatele mqweb server potřebuje určité oprávnění. Další informace naleznete v tématu Oprávnění požadované uživatelským ID úlohy mqweb serveru.

Zabezpečení-pomocí MQ Console a REST API

Použijete-li MQ Console a REST API, musíte se ověřit jako uživatel, který je zahrnut v nakonfigurovaném registru. Těmto uživatelům jsou přiřazeny specifické role, které určují akce, které mohou uživatelé provádět. Chcete-li například použít produkt messaging REST API, musí být uživateli přiřazena role `MQWebUser` . Další informace o dostupných rolích pro MQ Console a REST APIa o přístupu, který tyto role poskytují, najdete v tématu Role na MQ Console a REST API.

Další informace o konfiguraci zabezpečení pro produkty MQ Console a REST APInaleznete v tématu ZabezpečeníMQ Console a REST API.

Poznámky

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LICENČNÍ INFORMACE:

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

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

Informace o programovacím rozhraní

Informace programátorských rozhraní, jsou-li poskytovány, jsou určeny k tomu, aby vám pomohly vytvořit aplikační software pro použití s tímto programem.

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

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

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

Ochranné známky

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

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

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

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

Tento produkt obsahuje software vyvinutý v rámci projektu Eclipse Project (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: