

8.0

Konfigurace produktu IBM MQ

IBM

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí [“Poznámky” na stránce 635](#).

Toto vydání se vztahuje na verzi 8 vydání IBM® MQ a na všechna následná vydání a modifikace, dokud nebude v nových vydáních uvedeno jinak.

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

© **Copyright International Business Machines Corporation 2007, 2023.**

Obsah

Konfigurace.....	5
Vytváření a údržba správců front na distribuovaných platformách.....	5
Vytvoření výchozího správce front.....	8
Nastavení výchozího správce front jako výchozího správce front.....	9
Zálohování konfiguračních souborů po vytvoření správce front.....	10
Spuštění správce front.....	11
Zastavení správce front.....	11
Restartování správce front.....	13
Odstranění správce front.....	13
Konfigurace připojení mezi serverem a klientem.....	14
Který typ komunikace použít.....	16
Konfigurace rozšířeného transakčního klienta.....	18
Definování kanálů MQI.....	28
Vytvoření a použití kanálů AMQP.....	29
Vytváření připojení k serveru a připojení klienta na různých platformách.....	34
Vytvoření připojení k serveru a připojení klienta na serveru.....	37
Programy pro ukončení kanálů pro kanály MQI.....	42
Připojení klienta ke skupině sdílení front.....	46
Konfigurace klienta pomocí konfiguračního souboru.....	47
Použití proměnných prostředí IBM MQ.....	71
Změna konfiguračních informací IBM MQ a správce front.....	81
Změna konfiguračních informací v systémech Windows, SYSTÉM UNIX a Linux.....	81
Změna konfiguračních informací v systému IBM i.....	87
Atributy pro změnu konfiguračních informací IBM MQ.....	98
Změna konfiguračních informací správce front.....	105
Konfigurace distribuovaných front.....	124
IBM MQ technologie distribuovaných front.....	124
Úvod do distribuované správy front.....	143
Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux.....	173
Monitorování a řízení kanálů v systému IBM i.....	195
Konfigurace klastru správce front.....	216
Konfigurace publikování/odběru zpráv.....	329
Nastavení atributů zpráv publikování/odběru ve frontě.....	329
Spouštění publikování/odběru ve frontě.....	330
Zastavení publikování/odběru ve frontě.....	331
Přidání proudu.....	331
Odstranění proudu.....	332
Přidání bodu odběru.....	333
Konfigurace sítí distribuovaných publikování/odběru.....	334
Konfigurace více instalací.....	352
Připojování aplikací v prostředí s více instalačními prostředí.....	352
Změna primární instalace.....	360
Přidružení správce front k instalaci.....	362
Vyhledání instalací produktu IBM MQ v systému.....	363
Dostupnost, obnova a restartování.....	364
Automatické opětovné připojení klienta.....	365
Monitorování zpráv konzoly.....	371
Použití produktu IBM MQ s konfiguracemi vysoké dostupnosti.....	375
Ujištění se, že zprávy nejsou ztraceny (protokolování).....	457
Zálohování a obnova dat správce front produktu IBM MQ.....	475
Konfigurace prostředků produktu JMS.....	480
Konfigurace továren připojení a míst určení v oboru názvů JNDI.....	481

Konfigurace objektů produktu JMS pomocí produktu MQ Explorer.....	485
Konfigurace objektů produktu JMS pomocí nástroje pro administraci.....	486
Konfigurace prostředků produktu JMS v produktu WebSphere Application Server.....	495
Konfigurace aplikačního serveru pro použití nejnovější úrovně údržby adaptéru prostředků.....	502
Konfigurace vlastnosti produktu JMS PROVIDERVERSION	505
Odebrání trvalých odběrů produktu WebSphere Application Server verze 7 a verze 8.....	513
Konfigurace produktu HP Integrity NonStop Server.....	515
Přehled procesu brány.....	516
Konfigurace brány pro spuštění pod cestou Pathway.....	516
Konfigurace inicializačního souboru klienta.....	518
Udělení oprávnění pro kanály.....	518
Konfigurace produktu IBM MQ pomocí nástroje Docker.....	518
Podpora Docker na systémech Linux.....	518
Plánování vlastního obrazu správce front produktu IBM MQ pomocí nástroje Docker.....	519
Sestavení ukázkového obrazu správce front produktu IBM MQ pomocí nástroje Docker	520
Konfigurace správců front v systému z/OS.....	523
Příprava na přizpůsobení správců front produktu IBM MQ for z/OS.....	523
přizpůsobení IBM MQ for z/OS.....	528
Testování správce front v systému z/OS.....	582
Nastavení komunikace s ostatními správci front.....	590
Použití IBM MQ s IMS.....	619
Použití IBM MQ s CICS.....	627
Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services.....	627
Použití uživatelských procedur OTMA v produktu IMS.....	630
Poznámky	635
Informace o programovacím rozhraní.....	636
Ochranné známky.....	636

Konfigurace

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

Před konfigurací produktu IBM MQ si přečtěte informace o koncepcích produktu IBM MQ v příručce [IBM MQ Technical overview](#). Přečtěte si o tom, jak plánovat své prostředí IBM MQ v [Plánování](#).

Existuje řada různých metod, které můžete použít k vytvoření, konfiguraci a administraci správců front a jejich souvisejících prostředků v produktu IBM MQ. Tyto metody zahrnují rozhraní příkazového řádku, grafické uživatelské rozhraní a rozhraní API administrace. Další informace o těchto rozhraních naleznete v tématu [Administrace produktu IBM MQ](#).


Pokyny, jak vytvořit, spustit, zastavit a odstranit správce front, naleznete v tématu [“Vytváření a údržba správců front na distribuovaných platformách”](#) na stránce 5.

Informace o tom, jak vytvořit komponenty potřebné k propojení vašich instalací a aplikací produktu IBM MQ, najdete v tématu [“Konfigurace distribuovaných front”](#) na stránce 124.

Pokyny, jak připojit klienty k serveru IBM MQ pomocí různých metod, najdete v tématu [“Konfigurace připojení mezi serverem a klientem”](#) na stránce 14.

Pokyny pro konfiguraci klastru správců front naleznete v tématu [“Konfigurace klastru správců front”](#) na stránce 216.

Chování produktu IBM MQ nebo správce front můžete změnit změnou konfiguračních informací. Další informace viz [“Změna konfiguračních informací IBM MQ a správce front”](#) na stránce 81. Obecně není třeba restartovat správce front, aby se změny konfigurace projeví, kromě případu, kdy je uvedena v této dokumentaci k produktu.

 Pokyny pro konfiguraci prostoru IBM MQ for z/OS naleznete v příručce [“Konfigurace správců front v systému z/OS”](#) na stránce 523.

Související pojmy

[“Konfigurace správců front v systému z/OS”](#) na stránce 523

Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Související informace

[IBM MQ Technický přehled](#)

[Správa lokálních objektů produktu IBM MQ](#)

[Správa vzdálených objektů produktu IBM MQ](#)

 [Správa serveru IBM i](#)

 [Správa serveru IBM MQ for z/OS](#)

[Naplánování](#)

 [Plánování vašeho prostředí IBM MQ na systému z/OS](#)

Vytváření a údržba správců front na distribuovaných platformách

Než budete moci používat zprávy a fronty, musíte vytvořit a spustit alespoň jednoho správce front a jeho přidružené objekty.

Vytvoření správce front

Správce front spravuje prostředky, které jsou k ní přidruženy, zejména fronty, které vlastní. Poskytuje aplikacím pro volání rozhraní MQI (Message Queuing Interface) volání příkazů a příkazy k vytvoření, úpravě, zobrazení a odstranění objektů IBM MQ.

Chcete-li vytvořit správce front, použijte řídicí příkaz IBM MQ **crtmqm** (popsán v části **crtmqm**). Příkaz **crtmqm** automaticky vytvoří požadované výchozí objekty a systémové objekty (popsané v tématu **Systémové výchozí objekty**). Výchozí objekty tvoří základ všech definic objektů, které vytvoříte; systémové objekty jsou vyžadovány pro operaci správce front. Pokud jste vytvořili správce front a jeho objekty, spusťte správce front pomocí příkazu **strmqm**.

Poznámka: Produkt IBM MQ nepodporuje názvy počítačů, které obsahují mezery. Pokud instalujete produkt IBM MQ na počítač s názvem počítače, který obsahuje mezery, nemůžete vytvořit žádné správce front.

Než budete moci vytvořit správce front, je třeba zvážit několik bodů (zejména v produkčním prostředí). Postupujte podle následujícího kontrolního seznamu:

Instalace přidružená ke správci front

Příkaz **crtmqm** automaticky asociuje správce front s instalací, ze které byl příkaz **crtmqm** zadán. Pro příkazy, které pracují se správcem front, je třeba zadat příkaz z instalace přidružené ke správci front. Pomocí příkazu **setmqm** můžete změnit přidruženou instalaci správce front. Všimněte si, že instalační program produktu Windows nepřidává uživatele, který provádí instalaci do skupiny mqm, další podrobnosti viz [Oprávnění ke správě produktu IBM MQ v systémech UNIX, Linux® a Windows](#).

Konvence pojmenování

V názvech používejte velká písmena, aby byla možná komunikace se správcem front na všech platformách. Nezapomeňte, že názvy jsou přiřazovány přesně tak, jak je zadáte. Abyste se vyhnuli nepříjemnosti při psaní, nepoužívejte zbytečně dlouhé názvy.

Zadejte jedinečný název správce front.

Při vytváření správce front se ujistěte, že žádný jiný správce front nemá ve vaší síti stejný název *kdekoli*. Názvy správců front nejsou kontrolovány při vytvoření správce front a názvy, které nejsou jedinečné, brání vytváření kanálů pro distribuované fronty. Pokud používáte také síť pro zaslání zpráv publikování/odběru, jsou odběry asociovány s názvem správce front, který je vytvořil. Proto mohou správci front v klastru nebo v hierarchii mít stejný název, což může vést k tomu, že se k nim publikace nedostanou.

Jedním způsobem, jak zajistit jedinečnost, je předpona každého názvu správce front s vlastním jedinečným názvem uzlu. Je-li například uzel nazýván ACCOUNTS, můžete pojmenovat správce front ACCOUNTS.SATURN.QUEUE.MANAGER, kde SATURN identifikuje určitého správce front a QUEUE.MANAGER je rozšíření, které můžete poskytnout všem správcům front. Případně můžete tuto skutečnost vynechat, ale všimněte si, že ACCOUNTS.SATURN a ACCOUNTS.SATURN.QUEUE.MANAGER jsou *různé* názvy správců front.

Používáte-li produkt IBM MQ pro komunikaci s jinými podniky, můžete také jako předponu zahrnout také vlastní podnikový název. To se v příkladech nedějí, protože je ztíženo jejich sledování.

Poznámka: Názvy správců front v řídicích příkazech rozlišují velikost písmen. To znamená, že máte povoleno vytvořit dva správce front s názvy `jupiter.queue.manager` a `JUPITER.queue.manager`. Nicméně, je lepší se vyhnout takovým komplikacím.

Omezit počet správců front

Jako prostředky můžete vytvořit tolik správců front. Avšak protože každý správce front vyžaduje své vlastní prostředky, je obecně lepší mít jednoho správce front se 100 frontami v uzlu, než má deset správců front, každý z nich má deset front.

V produkčních systémech může být mnoho procesorů využíváno s jedním správcem front, ale větší serverové počítače mohou být spuštěny efektivněji s více správci front.

Určit výchozího správce front

Každý uzel by měl mít výchozího správce front, i když je možné nakonfigurovat IBM MQ na uzlu bez jednoho. Výchozí správce front je správce front, ke kterému se aplikace připojují, pokud ve volání MQCONN neurčí název správce front. Jedná se také o správce front, který zpracovává příkazy MQSC při vyvolání příkazu `runmqsc` bez zadání názvu správce front.

Zadání správce front jako výchozí hodnoty *nahrazuje* všechny existující výchozí specifikace správce front pro daný uzel.

Změna výchozí správy fronty může ovlivnit ostatní uživatele nebo aplikace. Změna nemá žádný vliv na aktuálně připojené aplikace, protože je může použít v rámci původního volání MQI v rámci dalších volání MQI. Tento manipulátor zajišťuje, aby byla volání směřována do stejného správce front. Veškeré aplikace, které se připojují po , změnily jste výchozí připojení správce front k novému výchozímu správci front. To může být to, co jste zamýšleli, ale měli byste to vzít v úvahu, dříve než změníte předvolbu.

Vytvoření výchozího správce front je popsáno v tématu [“Vytvoření výchozího správce front”](#) na stránce 8.

Určit frontu nedoručených zpráv

Fronta nedoručených zpráv je lokální fronta, do které jsou odesílány zprávy, pokud je nelze směřovat na zamýšlené místo určení.

Frontu nedoručených zpráv je důležité definovat pro každého správce front v dané síti. Pokud ji nedefinujete, chyby v aplikačních programech mohou způsobit uzavření kanálů a nemusí dojít k příjmu odpovědí na administrační příkazy.

Pokud se například aplikace pokusí vložit zprávu do fronty do jiného správce front, ale vydá špatný název fronty, kanál se zastaví a zpráva zůstane na přenosové frontě. Ostatní aplikace pak nemohou tento kanál používat pro své zprávy.

Kanály nemají vliv na to, zda mají správci front fronty nedoručených zpráv. Nedoručená zpráva je vložena do fronty nedoručených zpráv na přijímajícím konci, takže kanál a jeho přenosová fronta jsou k dispozici.

Při vytváření správce front je třeba pomoci příznaku -u zadat název fronty nedoručených zpráv. Příkaz MQSC můžete také použít ke změně atributů správce front, kterého jste již definovali, pro určení fronty nedoručených zpráv, která má být použita. Příklad příkazu MQSC ALTER naleznete v tématu [Práce se správci front](#) .

Určit výchozí přenosovou frontu

Přenosová fronta je lokální fronta, na které jsou zprávy v režimu přenosu na vzdáleného správce front řazeny před přenosem ve frontě. Výchozí přenosová fronta je fronta, která bude použita v případě, že není výslovně definována žádná přenosová fronta. Každému správci front lze přiřadit výchozí přenosovou frontu.

Při vytváření správce front použijte příznak -d k určení názvu výchozí přenosové fronty. Ve skutečnosti to ve skutečnosti nevytvoří frontu; musíte to udělat výslovně později. Další informace naleznete v tématu [Práce s lokálními frontami](#) .

Uveďte parametry protokolování, které požadujete

Můžete určit parametry protokolování u příkazu `crtmqm` , včetně typu protokolování a cesty a velikosti souborů protokolu.

Ve vývojovém prostředí by měly být výchozí parametry protokolování vhodné. Výchozí hodnoty však můžete změnit, pokud například:

- Máte nízkokoncovou konfiguraci systému, která nemůže podporovat velké protokoly.
- Předpokládáte velký počet dlouhých zpráv ve frontách současně.
- Předpokládáte velké množství trvalých zpráv, které procházejí správcem front.

Jakmile nastavíte parametry protokolování, některé z nich lze změnit pouze odstraněním správce front a jeho opětovným vytvořením se stejným názvem, ale s různými parametry protokolování.

Další informace o parametrech protokolování viz [“Dostupnost, obnova a restartování”](#) na stránce 364.

UNIX

Pouze pro systémy IBM MQ for UNIX

Před použitím příkazu `crtmqm` můžete vytvořit adresář správce front `/var/mqm/qmgrs/<qmgr>`, a to dokonce i v samostatném lokálním systému souborů. Pokud použijete volbu `crtmqm` , pokud existuje adresář `/var/mqm/qmgrs/<qmgr>` , je prázdný a je vlastněn `mqm`, používá se pro data správce front. Není-li adresář vlastněn `mqm`, vytvoření selže se zprávou First Failure Support Technology (FFST). Pokud adresář není prázdný, vytvoří se nový adresář.

Související pojmy

[“Konfigurace správců front v systému z/OS” na stránce 523](#)

Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

[“Konfigurace” na stránce 5](#)

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

[“Zálohování konfiguračních souborů po vytvoření správce front” na stránce 10](#)

Konfigurační informace produktu IBM MQ jsou uloženy v konfiguračních souborech v systémech Windows, SYSTÉM UNIX a Linux .

[“Spuštění správce front” na stránce 11](#)

Při vytváření správce front je nutné jej spustit, aby bylo možné ji povolit pro zpracování příkazů nebo volání MQI.

[“Zastavení správce front” na stránce 11](#)

Existují tři způsoby, jak zastavit správce front: klidové ukončení a okamžité ukončení práce systému a preventivní ukončení práce.

[“Restartování správce front” na stránce 13](#)

Pomocí příkazu **strmqm** lze znovu spustit správce front nebo v systémech IBM MQ for Windows a IBM MQ pro systémy Linux x86-64 restartovat správce front z produktu IBM MQ Explorer.

[“Změna konfiguračních informací IBM MQ a správce front” na stránce 81](#)

Změňte chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související úlohy

[“Nastavení výchozího správce front jako výchozího správce front” na stránce 9](#)

Můžete vytvořit existujícího správce front jako výchozího správce front. Způsob, jakým to provedete, závisí na použité platformě.

[“Odstranění správce front” na stránce 13](#)

Správce front můžete odstranit pomocí příkazu **dltmqm** nebo pomocí Průzkumníka IBM MQ .

Související informace

[Vytvoření správce front s názvem QM1](#)


[Systémové a výchozí objekty](#)

Vytvoření výchozího správce front

Výchozí správce front je správce front, ke kterému se aplikace připojují, pokud nespecifikují název správce front v rámci volání MQCONN. Jedná se také o správce front, který zpracovává příkazy MQSC při vyvolání příkazu **runmqsc** bez zadání názvu správce front. Chcete-li vytvořit správce front, použijte řídicí příkaz IBM MQ **crtmqm**.

Než začnete

Před vytvořením výchozího správce front si přečtěte informace popsané v tématu [“Vytváření a údržba správců front na distribuovaných platformách” na stránce 5.](#)

 Pokud k vytvoření správce front v produktu UNIX používáte produkt **crtmqm** , je v případě, že adresář `/var/mqm/qmgrs/<qmgr>` již existuje, vlastníkem `mqm` a je prázdný, používá se pro data správce front. Pokud adresář není vlastněn `mqm`, vytvoření správce front selže se zprávou First Failure Support Technology (FFST). Není-li adresář prázdný, vytvoří se nový adresář pro data správce front.

Tato úvaha platí i v případě, že adresář `/var/mqm/qmgrs/<qmgr>` již existuje na samostatném lokálním systému souborů.

Informace o této úloze

Vytvoříte-li správce front pomocí příkazu **crtmqm**, příkaz automaticky vytvoří požadované výchozí objekty a systémové objekty. Výchozí objekty tvoří základ všech definic objektů, které zpřístupníte, a systémové objekty jsou vyžadovány pro operaci správce front.

Zadáním příslušných parametrů v příkazu můžete také definovat například název výchozí přenosové fronty, která má být použita správcem front, a název fronty nedoručených zpráv.

Windows V systému Windows můžete použít volbu **sax** příkazu **crtmqm** ke spuštění více instancí správce front.

Další informace o příkazu **crtmqm** a jeho syntaxi naleznete v tématu [crtmqm](#).

Procedura

- Chcete-li vytvořit výchozího správce front, použijte příkaz **crtmqm** s parametrem **-q**.

Následující příklad příkazu **crtmqm** vytvoří výchozího správce front s názvem SATURN.QUEUE.MANAGER:

```
crtmqm -q -d MY.DEFAULT.XMIT.QUEUE -u SYSTEM.DEAD.LETTER.QUEUE SATURN.QUEUE.MANAGER
```

kde:

-q

Označuje, že tento správce front je výchozím správcem front.

-d MY.DEFAULT.XMIT.QUEUE

Představuje název výchozí přenosové fronty, kterou má tento správce front použít.

Poznámka: IBM MQ nevytvoří výchozí přenosovou frontu pro sebe; musíte ji definovat sami.

-u SYSTEM.DEAD.LETTER.QUEUE

Název výchozí fronty pro dead-letter vytvořeného produktem IBM MQ při instalaci.

SATURN.QUEUE.MANAGER

Jedná se o název tohoto správce front. Musí se jednat o poslední parametr zadaný v příkazu **crtmqm**.

Jak pokračovat dále

Pokud jste vytvořili správce front a jeho objekty, použijte příkaz **stmqm** ke spuštění správce front.

Související pojmy

[“Zálohování konfiguračních souborů po vytvoření správce front” na stránce 10](#)

Konfigurační informace produktu IBM MQ jsou uloženy v konfiguračních souborech v systémech Windows, SYSTÉM UNIX a Linux.

Související informace

[Práce se správcem front](#)

[Práce s lokálními frontami](#)

[Systémové a výchozí objekty](#)

Nastavení výchozího správce front jako výchozího správce front

Můžete vytvořit existujícího správce front jako výchozího správce front. Způsob, jakým to provedete, závisí na použité platformě.

Systemy IBM MQ for Windows a IBM MQ for Linux (platformy x86 a x86-64)

Informace o této úloze

Chcete-li vytvořit existujícího správce front jako výchozího správce front v systémech IBM MQ for Windows a IBM MQ pro platformy Linux (platformy x86 a x86-64), postupujte podle následujících pokynů:

Postup

1. Otevřete Průzkumníka IBM MQ .
2. Klepněte pravým tlačítkem myši na IBM WebSphere MQ a pak vyberte Properties Zobrazí se panel Vlastnosti pro IBM MQ .
3. Do pole Výchozí název správce front zadejte název výchozího správce front.
4. Klepněte na tlačítko OK.

Systemy SYSTÉM UNIX a Linux

Informace o této úloze

Při vytváření výchozího správce front je jeho název vložen do atributu Name stanzy `DefaultQueueManager` v konfiguračním souboru IBM MQ (`mqs.ini`). Stanza a její obsah se automaticky vytvoří, pokud neexistují.

Procedura

- Chcete-li existující správce front změnit jako výchozí, změňte název správce front v atributu Name na název nového výchozího správce front. To můžete provést ručně pomocí textového editoru.
- Nemáte-li na uzlu výchozího správce front a chcete vytvořit existující správce front jako výchozí, vytvořte objekt stanza `DefaultQueueManager` se požadovaným názvem.
- Pokud omylem uděláte jiného správce front jako výchozí a chcete se vrátit k původnímu výchozímu správci front, upravte sekci `DefaultQueueManager` v souboru `mqs.inia` nahraďte nechtěného výchozího správce front tím, co chcete.

Jak pokračovat dále

Informace o konfiguračních souborech viz [“Změna konfiguračních informací IBM MQ a správce front”](#) na stránce 81 .

Zálohování konfiguračních souborů po vytvoření správce front

Konfigurační informace produktu IBM MQ jsou uloženy v konfiguračních souborech v systémech Windows, SYSTÉM UNIX a Linux .

V systémech Windows a Linux (x86 a x86-64) používají systémy MQ Explorer k provádění změn v konfiguračních souborech.

Na systémech Windows můžete také použít příkaz `amqmdain` k provedení změn v konfiguračních souborech. Viz, [amqmdain](#)

Existují dva typy konfiguračního souboru:

- Když instalujete produkt, vytvoří se konfigurační soubor IBM MQ (`mqs.ini`). Obsahuje seznam správců front, kteří jsou aktualizováni při každém vytvoření nebo odstranění správce front. Pro každý uzel je k dispozici jeden soubor `mqs.ini` .
- Při vytváření nového správce front je automaticky vytvořen nový konfigurační soubor správce front (`qm.ini`). Obsahuje konfigurační parametry pro správce front.

V 8.0.0.4 Pokud jste nainstalovali službu AMQP, pak existuje další konfigurační soubor, který musíte zálohovat:

- `amqp_win.properties` (Windows)
- `amqp_unix.properties` (UNIX/Linux)

Po vytvoření správce front zazálohujte své konfigurační soubory. Pokud pak vytvoříte jiného správce front, který způsobuje problémy, můžete zálohy obnovit, až odeberete zdroj daného problému. Obecně platí, že při každém vytvoření nového správce front zálohujte své konfigurační soubory.

Další informace o konfiguračních souborech viz [“Změna konfiguračních informací IBM MQ a správce front”](#) na stránce 81.

Spuštění správce front

Při vytváření správce front je nutné jej spustit, aby bylo možné ji povolit pro zpracování příkazů nebo volání MQI.

Chcete-li spustit správce front, použijte příkaz **strmqm**.

Poznámka: Příkaz **strmqm** je třeba použít z instalace přidružené ke správci front, se kterým pracujete. Pomocí příkazu `dspmqr -o installation` můžete zjistit, která instalace správce front je přidružena.

Chcete-li například spustit správce front QMB, zadejte tento příkaz:

```
strmqm QMB
```

Na systémech IBM MQ for Windows a IBM MQ for Linux (platformy x86 a x86-64) můžete spustit správce front následujícím způsobem:

1. Otevřete Průzkumníka IBM MQ.
2. Vyberte správce front z pohledu Navigator.
3. Klepněte na tlačítko Start. Spustí se správce front.

Pokud spuštění správce front trvá déle než několik sekund, produkt IBM MQ vyšle informační zprávy přerušovaně podrobně popisující průběh spouštění.

Příkaz `strmqm` nevrací řízení, dokud nebude správce front spuštěn a je připraven přijímat požadavky na připojení.

Automatické spuštění správce front

V produktu IBM MQ for Windows můžete správce front spustit automaticky, když se systém spustí pomocí Průzkumníka IBM MQ. Další informace najdete v tématu [Administrace pomocí produktu MQ Explorer](#).

Zastavení správce front

Existují tři způsoby, jak zastavit správce front: klidové ukončení a okamžité ukončení práce systému a preventivní ukončení práce.

Chcete-li zastavit správce front, použijte příkaz **endmqm**.

Poznámka: Příkaz **endmqm** je třeba použít z instalace přidružené ke správci front, se kterým pracujete. Pomocí příkazu `dspmqr -o installation` můžete zjistit, která instalace správce front je přidružena.

Chcete-li například zastavit správce front s názvem QMB, zadejte následující příkaz:

```
endmqm QMB
```

V systémech IBM MQ for Windows a IBM MQ for Linux (platformy x86 a x86-64) můžete správce front zastavit následujícím způsobem:

1. Otevřete Průzkumníka IBM MQ .
2. Vyberte správce front z pohledu Navigator .
3. Klepněte na tlačítko Stop Zobrazí se panel Ukončení správce front.
4. Vyberte Řízený, nebo Okamžitě.
5. Klepněte na tlačítko OK . Správce front je zastaven.

klidové ukončení

Příkaz **endmqm** standardně provádí klidové ukončení běhu zadaného správce front. Dokončení této operace může trvat určitou dobu. Do klidového stavu bylo ukončeno, dokud se všechny připojené aplikace neodpojí.

Tento typ ukončení práce systému můžete použít k zastavení aplikací. Pokud zadáte:

```
endmqm -c QMB
```

není vám řečeno, kdy byly zastaveny všechny aplikace. (Příkaz **endmqm -c QMB** je ekvivalentní příkazu **endmqm QMB** .)

Nicméně, pokud zadáte:

```
endmqm -w QMB
```

příkaz čeká, dokud všechny aplikace nebudou zastaveny a správce front ukončen.

okamžité ukončení práce systému

Okamžité ukončení činnosti aktuálních volání MQI lze dokončit, ale všechny nové volání se nezdaří. Tento typ ukončení činnosti nečeká, až se aplikace odpojí od správce front.

Chcete-li provést okamžité ukončení práce, zadejte:

```
endmqm -i QMB
```

preventivní ukončení

Poznámka: Tuto metodu nepoužívejte, pokud se nezdaří všechny ostatní pokusy o zastavení správce front pomocí příkazu **endmqm** . Tato metoda může mít nepředvídatelné důsledky pro připojené aplikace.

Pokud okamžité ukončení práce nefunguje, musíte se uchýlit k ukončení *preemptivního* ukončení, přičemž byste měli zadat parametr -p . Příklad:

```
endmqm -p QMB
```

To okamžitě zastaví správce front. Pokud tato metoda stále nefunguje, přečtěte si téma [Ruční zastavení správce front](#) pro alternativní řešení.

Podrobný popis příkazu **endmqm** a jeho voleb naleznete v souboru [endmqm](#).

Máte-li problémy při ukončování práce správce front

Problémy při ukončování činnosti správce front jsou často způsobeny aplikacemi. Například, když aplikace:

- Nezaškrtnli správně návratové kódy MQI
- Nevyžadovat oznámení o uvedení do klidového stavu
- Ukončit bez odpojení od správce front (zadáním volání MQDISC)

Pokud se vyskytne problém při zastavení správce front, můžete příkaz **endmqm** přerušit pomocí Ctrl-C. Poté můžete zadat jiný příkaz **endmqm**, ale tentokrát s příznakem, který určuje typ ukončení práce, který vyžadujete.

Restartování správce front

Pomocí příkazu **strmqm** lze znovu spustit správce front nebo v systémech IBM MQ for Windows a IBM MQ pro systémy Linux x86-64 restartovat správce front z produktu IBM MQ Explorer.

Chcete-li restartovat správce front, zadejte příkaz:

```
strmqm saturn.queue.manager
```

V systémech IBM MQ for Windows a IBM MQ pro systémy Linux x86-64 můžete správce front restartovat stejným způsobem, jako jeho spuštění, jak je uvedeno níže:

1. Otevřete Průzkumníka IBM MQ .
2. Vyberte správce front z pohledu Navigator .
3. Klepněte na tlačítko Start . Správce front se restartuje.

Pokud restart správce front trvá déle než několik sekund, IBM MQ zobrazí informační zprávy s přerušovaným podrobným popisem průběhu spouštění.

Odstranění správce front

Správce front můžete odstranit pomocí příkazu **dltmqm** nebo pomocí Průzkumníka IBM MQ .

Než začnete

Zastavte správce front.

Procedura

- Spusťte následující příkaz: `dltmqm QMB`

Poznámka: Příkaz **dltmqm** je třeba použít z instalace přidružené ke správci front, se kterým pracujete. Pomocí příkazu `dspmqr -o installation` můžete zjistit, která instalace správce front je přidružena.

Postup odstranění správce front

Informace o této úloze

V systémech IBM MQ for Windows a IBM MQ for Linux (platformyx86 a x86-64) můžete správce front odstranit následujícím způsobem:

Postup

1. Otevřete Průzkumníka IBM MQ .
2. V pohledu Navigator vyberte správce front.
3. Není-li správce front zastaven, zastavte jej.
 - a) Klepněte pravým tlačítkem myši na správce front.
 - b) Klepněte na tlačítko **Zastavit**.
4. Klepněte pravým tlačítkem myši na správce front.
5. Klepněte na tlačítko **Odstranit**.

Výsledky

Správce front je odstraněn.



Upozornění:

- Odstranění správce front je drastický krok, protože také odstraní všechny prostředky přidružené ke správci front, včetně všech front a jejich zpráv a všech definic objektů. Pokud použijete příkaz **dltmqm**, nezobrazí se žádná výzva, která vám umožní změnit svou mysl; když stisknete klávesu Enter, všechny přidružené prostředky se ztratí.
- V produktu IBM MQ for Windows správce front také odebere správce front ze seznamu automatického spouštění (popsaného v tématu [“Spuštění správce front”](#) na stránce 11). Po dokončení příkazu se zobrazí zpráva IBM MQ queue manager ending. Nesdělili jste, že správce front byl odstraněn.
- Odstranění správce front klastru ji neodebere z klastru. Další informace viz poznámka v popisu **dltmqm**.

Pro popis příkazu **dltmqm** a jeho voleb viz [dltmqm](#). Ujistěte se, že oprávnění k použití tohoto příkazu má pouze důvěryhodní administrátoři. (Informace o zabezpečení najdete v tématu [Nastavení zabezpečení](#) v systémech Windows, SYSTÉM UNIX a Linux.)

Konfigurace připojení mezi serverem a klientem

Chcete-li nakonfigurovat komunikační propojení mezi IBM MQ MQI clients a servery, rozhodněte se v komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

V produktu IBM MQ se odkazy logických komunikací mezi objekty nazývají *kanály*. Kanály použité pro připojení IBM MQ MQI clients k serverům se nazývají kanály MQI. Definice kanálů nastavíte na každém konci své vazby tak, aby aplikace IBM MQ na serveru IBM MQ MQI client mohla komunikovat se správcem front na serveru. Podrobný popis postupu naleznete v tématu [Uživatelské kanály definované uživatelem](#).

Před definováním kanálů modulu MQI je třeba provést následující akce:

1. Rozhodněte se na způsob komunikace, který budete používat. Viz [“Který typ komunikace použít”](#) na stránce 14.
2. Definujte připojení na každém konci kanálu:

Chcete-li definovat připojení, musíte:

- Nakonfigurujte připojení.
- Poznamenejte si hodnoty parametrů, které potřebujete pro definice kanálů.
- Povolte serveru, aby zjistil příchozí síťové požadavky ze svého serveru IBM MQ MQI clientspuštěním modulu *listener*.

Který typ komunikace použít





Různé platformy podporují různé přenosové protokoly. Výběr přenosového protokolu závisí na vaší kombinaci IBM MQ MQI client a platform serverů.

Pro kanály MQI jsou k dispozici až čtyři typy přenosových protokolů v závislosti na vašich klientských a serverových platformách:

- LU 6.2
- NetBIOS
- SPX
- Protokol TCP/IP

Definujete-li kanály MQI, musí každá definice kanálu určovat atribut přenosového protokolu (typ transportu). Server není omezen na jeden protokol, takže různé definice kanálů mohou určovat různé protokoly. Pro produkt IBM MQ MQI clients může být užitečné používat alternativní kanály MQI s použitím různých přenosových protokolů.





Výběr přenosového protokolu může být omezen vaší konkrétní kombinací platform IBM MQ MQI client a serverů. Možné kombinace jsou uvedeny v následující tabulce.

Tabulka 1. Přenosové protokoly-kombinace IBM MQ MQI client a serverových platform		
Přenosový protokol	IBM MQ MQI client	Server IBM MQ
Protokol TCP/IP	 IBM i Systémy UNIX Windows	 IBM i Systémy UNIX Windows z/OS
LU 6.2	Systémy UNIX ¹ Windows	 IBM i Systémy UNIX ¹ Windows  z/OS
NetBIOS	Windows	Windows
SPX	Windows	Windows

Poznámka:

1. Kromě Linux pro Power Systems

Další informace o nastavení různých typů připojení naleznete v následujících odkazech:

- [“limity připojení TCP/IP” na stránce 17](#)
- [“Definování připojení TCP na systému Windows” na stránce 183](#)
- [“Definování připojení TCP na systému SYSTÉM UNIX a Linux” na stránce 190](#)
-  [“Definování připojení TCP na systému IBM i” na stránce 210](#)
-  [“Definování připojení TCP na systému z/OS” na stránce 611](#)
- [“Definování připojení LU 6.2 na systému Windows” na stránce 185](#)
- [“Definování připojení LU 6.2 na systému SYSTÉM UNIX a Linux” na stránce 194](#)
-  [“Definování připojení LU 6.2 na systému IBM i” na stránce 211](#)
-  [“Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS” na stránce 613](#)
- [“Definování připojení NetBIOS v systému Windows” na stránce 187](#)

Související pojmy

[“Konfigurace rozšířeného transakčního klienta” na stránce 18](#)

Tato kolekce témat popisuje, jak nakonfigurovat rozšířenou transakční funkci pro každou kategorii správce transakcí.

[“Definování kanálů MQI” na stránce 28](#)

Chcete-li vytvořit nový kanál, musíte vytvořit **dvě** definice kanálu, jeden pro každý konec připojení, a to pomocí stejného názvu kanálu a kompatibilních typů kanálů. V tomto případě jsou typy kanálů *server-připojení* a *připojení klienta*.

[“Vytváření připojení k serveru a připojení klienta na různých platformách” na stránce 34](#)

Můžete vytvořit každou definici kanálu na počítači, na který se vztahuje. Existují omezení, jak můžete vytvářet definice kanálů na klientském počítači.

[“Vytvoření připojení k serveru a připojení klienta na serveru” na stránce 37](#)

Na serveru můžete vytvořit obě definice a potom zpřístupnit definici klienta-připojení klientovi.

[“Programy pro ukončení kanálů pro kanály MQI” na stránce 42](#)

Pro prostředí IBM MQ MQI client v systémech UNIX, Linux a Windows jsou k dispozici tři typy ukončení kanálu.

[“Připojení klienta ke skupině sdílení front” na stránce 46](#)

Klienta lze připojit ke skupině sdílení front prostřednictvím vytvoření kanálu MQI mezi klientem a správcem front na serveru, který je členem skupiny sdílení front.

[“Konfigurace klienta pomocí konfiguračního souboru” na stránce 47](#)

Nakonfigurujte své klienty pomocí atributů v textovém souboru. Tyto atributy mohou být přepsány proměnnými prostředí nebo jinými způsoby specifickými pro platformu.

Související informace

[Připojení klientských aplikací IBM MQ MQI ke správcům front](#)

[ZOBRAZIT VELIKOST CHUSH](#)

[SET CHLAUTH](#)

Který typ komunikace použít

Různé platformy podporují různé komunikační protokoly. Výběr přenosového protokolu závisí na vaší kombinaci IBM MQ MQI client a platform serverů.

Pro kanály MQI na různých platformách existují čtyři typy komunikace:






- LU 6.2
- NetBIOS
- SPX
- Protokol TCP/IP

Definujete-li kanály MQI, musí každá definice kanálu určovat atribut přenosového protokolu (typ transportu). Server není omezen na jeden protokol, takže různé definice kanálů mohou určovat různé protokoly. Pro produkt IBM MQ MQI clients může být užitečné používat alternativní kanály MQI s použitím různých přenosových protokolů.

Volba přenosového protokolu závisí také na vaší konkrétní kombinaci klientských a serverových platform IBM MQ. Možné kombinace jsou uvedeny v následující tabulce.

Poznámka:

1. Kromě Linux (platforma POWER)

Přenosový protokol	IBM MQ MQI client	Server IBM MQ
Protokol TCP/IP	 IBM i Systémy UNIX Windows	 IBM i Systémy UNIX Windows  z/OS
LU 6.2	Systémy UNIX ¹ Windows	 IBM i Systémy UNIX ¹ Windows  z/OS
NetBIOS	Windows	Windows

Tabulka 2. Přenosové protokoly-kombinace klientských a serverových platforem IBM MQ (pokračování)

Přenosový protokol	IBM MQ MQI client	Server IBM MQ
SPX	Windows	Windows

Související pojmy

[“Definování připojení TCP na systému Windows”](#) na stránce 183

Definujte připojení TCP nakonfigurováním kanálu na odesílajícím konci, abyste určili adresu cíle, a spuštěním programu modulu listener na přijímajícím konci.

[“Definování připojení TCP na systému SYSTÉM UNIX a Linux”](#) na stránce 190

Definice kanálu na odesílajícím konci uvádí adresu cíle. Modul listener nebo démon inet je konfigurován pro připojení na konci příjmu.

[“Definování připojení TCP na systému IBM i”](#) na stránce 210

V rámci definice kanálu můžete definovat připojení TCP pomocí pole Název připojení.

[“Definování připojení TCP na systému z/OS”](#) na stránce 611

Chcete-li definovat připojení TCP, je zde několik nastavení, které je třeba nakonfigurovat.

[“Definování připojení LU 6.2 na systému Windows”](#) na stránce 185

Musí být konfigurována služba SNA, aby bylo možné mezi těmito dvěma počítači vytvořit konverzaci LU 6.2 .

[“Definování připojení LU 6.2 na systému SYSTÉM UNIX a Linux”](#) na stránce 194

Musí být konfigurována služba SNA, aby bylo možné mezi těmito dvěma počítači vytvořit konverzaci LU 6.2 .

[“Definování připojení LU 6.2 na systému IBM i”](#) na stránce 211

Definujte podrobnosti o komunikaci LU 6.2 pomocí názvu režimu, názvu TP a názvu připojení pro plně kvalifikované připojení LU 6.2 .

[“Definování připojení NetBIOS v systému Windows”](#) na stránce 187

Produkt IBM MQ používá tři typy prostředků NetBIOS při vytváření připojení NetBIOS k jinému produktu IBM MQ : relace, příkazy a názvy. Každý z těchto prostředků má limit, který je standardně nastaven buď standardně, nebo volbou během instalace NetBIOS.

Související odkazy

[“limity připojení TCP/IP”](#) na stránce 17

Počet neprovedených požadavků na připojení, které lze zařadit do fronty v jednom portu TCP/IP, závisí na platformě. Pokud je dosažen limit, dojde k chybě.

[“Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS”](#) na stránce 613

Chcete-li definovat připojení LU6.2 , je třeba nakonfigurovat několik nastavení.

Definování připojení TCP/IP

Určení typu transportu TCP v definici kanálu na straně klienta. Spusťte na serveru program modulu listener.

Určete připojení TCP/IP na straně klienta zadáním typu transportu TCP v definici kanálu.

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu. Chcete-li to provést, je třeba spustit program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Postup pro spuštění programu modulu listener závisí na platformě serveru.

Další informace naleznete v souvisejících tématech pro platformy klienta a serveru.

limity připojení TCP/IP

Počet neprovedených požadavků na připojení, které lze zařadit do fronty v jednom portu TCP/IP, závisí na platformě. Pokud je dosažen limit, dojde k chybě.

Toto omezení připojení není stejné jako maximální počet klientů, které lze připojit k serveru IBM MQ . Můžete připojit více klientů k serveru, až do úrovně určené systémovými prostředky serveru. Hodnoty nevyřízených požadavků pro požadavky na připojení jsou zobrazeny v následující tabulce:

Tabulka 3. Maximální počet nevyřízených požadavků na připojení zařazených do fronty na portu TCP/IP

Platforma serveru	Maximum požadavků na připojení
AIX	100
HP-UX	20
Linux	100
IBM	255
Solaris	100
Server Windows	100
Windows Pracovní stanice	100
z/OS	255

Je-li dosaženo limitu připojení, klient obdrží návratový kód MQRC_HOST_NOT_AVAILABLE z volání MQCONN a chybu AMQ9202 v protokolu chyb klienta (/var/mqm/errors/AMQERR0n . LOG na systémech SYSTÉM UNIX a Linux nebo amqerr0n . log v podadresáři chyb instalace klienta IBM MQ v systému Windows). Pokud se klient pokusí o požadavek MQCONN , může být úspěšný.

Chcete-li zvýšit počet požadavků na připojení, které můžete provést, a zabránit vzniku chybových zpráv generovaných tímto omezením, můžete mít více modulů listener, které naslouchají na odlišném portu, nebo které mají více než jednoho správce front.

Definování připojení NetBIOS

Připojení NetBIOS platí pouze pro systémy Windows .

Připojení NetBIOS se vztahuje pouze na klienta a server, na kterém je spuštěn produkt Windows. Viz [Definování připojení NetBIOS](#).

Konfigurace rozšířeného transakčního klienta

Tato kolekce témat popisuje, jak nakonfigurovat rozšířenou transakční funkci pro každou kategorii správce transakcí.

Pro každou platformu poskytuje rozšířený transakční klient podporu pro následující externí správce transakcí:

správci transakcí kompatibilní se standardem XA

Rozšířený transakční klient poskytuje rozhraní správce prostředků XA pro podporu správců transakcí s podporou standardu XA, jako je například produkt CICS a Tuxedo.

Microsoft Transaction Server (pouze systémy Windows)

Pouze v systémech Windows podporuje rozhraní správce prostředků XA také Microsoft Transaction Server (MTS). Podpora produktu IBM MQ MTS dodaná s rozšířeným transakčním klientem poskytuje most mezi MTS a rozhraním správce prostředků XA.

WebSphere Application Server

Starší verze produktu IBM MQ podporovaly WebSphere Application Server verze 4 nebo verze 5 a vyžadovaly, abyste provedli určité konfigurační úlohy, aby bylo možné používat rozšířeného transakčního klienta. WebSphere Application Server Produkt Verze 6 a dále obsahuje poskytovatele systému zpráv produktu IBM MQ , takže není třeba používat rozšířeného klienta transakcí.

Související pojmy

[“Konfigurace správců transakcí s podporou standardu XA” na stránce 19](#)

Nejprve nakonfigurujte základního klienta produktu IBM MQ a potom nakonfigurujte rozšířenou transakční funkci s použitím informací v těchto tématech.

[“Microsoft Transakční server” na stránce 27](#)

Před tím, než můžete použít MTS jako správce transakcí, není třeba žádná další konfigurace. Existují však body, které je třeba poznamenat.

Konfigurace správců transakcí s podporou standardu XA

Nejprve nakonfigurujte základního klienta produktu IBM MQ a potom nakonfigurujte rozšířenou transakční funkci s použitím informací v těchto tématech.

Poznámka: V tomto oddílu se předpokládá, že máte základní informace o rozhraní XA, které je publikováno skupinou Open Group v tématu *Distribuované zpracování transakcí: Specifikace XA*.

Chcete-li nakonfigurovat rozšířeného transakčního klienta, musíte nejprve nakonfigurovat základního klienta produktu IBM MQ, jak je popsáno v tématu *Instalace klienta IBM MQ*. Pomocí informací v této sekci pak můžete nakonfigurovat rozšířenou transakční funkci pro správce transakcí vyhovující standardu XA, jako je CICS a Tuxedo.

Správce transakcí komunikuje se správcem front jako správce prostředků s použitím stejného kanálu MQI jako správce front používaný aplikací klienta, která je připojena ke správci front. Když správce transakcí zavolá volání funkce správce prostředků (xa_), použije se kanál MQI k předání volání správci front a k přijetí výstupu zpět od správce front.

Správce transakcí může spustit kanál MQI zadáním volání xa_open pro otevření správce front jako správce prostředků, nebo může klientská aplikace spustit kanál MQI zadáním volání MQCONN nebo MQCONNX.

- Pokud správce transakcí spustí kanál MQI a klientská aplikace později zavolá volání MQCONN nebo MQCONNX na stejném podprocesu, volání MQCONN nebo MQCONNX se úspěšně dokončí a vrátí se popisovač připojení k aplikaci. Aplikace neobdrží kód dokončení MQCC_WARNING s kódem příčiny MQRC_ALREADY_CONNECTED.
- Pokud klientská aplikace spustí kanál MQI a správce transakcí později vyvolá řetězec xa_open ve stejném podprocesu, bude volání xa_open předáno správci front s použitím kanálu MQI.

Pokud v situaci zotavení po selhání nejsou spuštěny žádné klientské aplikace, může správce transakcí použít vyhrazený kanál MQI k obnovení všech nedokončených jednotek práce, v nichž se správce front účastnil v době selhání.

Všimněte si následujících podmínek, když používáte rozšířeného transakčního klienta se správcem transakcí kompatibilním s XA:

- V rámci jednoho podprocesu může být klientská aplikace připojena pouze k jednomu správci front v daném okamžiku. Toto omezení platí pouze v případě, že používáte rozšířeného transakčního klienta. Klientská aplikace, která používá základního klienta produktu IBM MQ, může být připojena k více než jednomu správci front souběžně v rámci jednoho podprocesu.
- Každý podproces aplikace klienta se může připojit k jinému správci front.
- Klientská aplikace nemůže používat sdílené obslužné rutiny připojení.

Chcete-li nakonfigurovat funkci rozšířených transakcí, je třeba pro každého správce front, který se chová jako správce prostředků, poskytnout následující informace:

- Řetězec xa_open
- Ukazatel na strukturu přepínačů XA

Když správce transakcí volá řetězec xa_open, aby otevřel správce front jako správce prostředků, předá řetězec xa_open k rozšířenému transakčnímu klientovi jako argument xa_infona volání. Rozšířený transakční klient používá informace v řetězci xa_open následujícími způsoby:

- Chcete-li spustit kanál MQI pro správce front serveru, pokud aplikace klienta dosud není spuštěna, spusťte ji.
- Chcete-li zkontrolovat, zda je správce front, kterého správce transakcí otevře jako správce prostředků, stejný jako správce front, ke kterému se připojuje klientská aplikace,

- Chcete-li vyhledat funkce ax_reg a ax_unreg správce transakcí, používá-li správce front dynamickou registraci,

Formát řetězce xa_open a další informace o tom, jak jsou informace v řetězci xa_open použity rozšířeným transakčním klientem, viz [“Formát řetězce xa_open”](#) na stránce 21.

Struktura přepínačů XA umožňuje správci transakcí vyhledat funkce transakce _ funkce poskytované rozšířeným transakčním klientem a určuje, zda správce front používá dynamickou registraci. Informace o strukturách přepínačů XA dodaných s rozšířeným transakčním klientem najdete v tématu [“Struktury přepínačů XA”](#) na stránce 24.

Informace o tom, jak nakonfigurovat rozšířenou transakční funkci pro určitého správce transakcí, a další informace o použití správce transakcí s rozšířeným transakčním klientem najdete v následujících sekcích:

- [“Konfigurace rozšířeného transakčního klienta pro produkt CICS”](#) na stránce 26
- [“Konfigurace rozšířeného transakčního klienta pro Tuxedo”](#) na stránce 27

Související pojmy

[“Parametry CHANNEL, TRPTYPE, CONNAME a QMNAME řetězce xa_open”](#) na stránce 23

Tyto informace vám pomohou pochopit, jak rozšířený transakční klient používá tyto parametry k určení správce front, k němuž se má připojit.

[“Další zpracování chyb pro xa_open”](#) na stránce 24

Volání xa_open selhává za určitých okolností.

Související úlohy

[“Použití rozšířeného transakčního klienta s kanály SSL”](#) na stránce 25

Pomocí řetězce xa_open nelze nastavit kanál SSL. Postupujte podle těchto pokynů, chcete-li použít tabulku definic kanálů klienta (ccdt).

Související odkazy

[“Parametry TPM a AXLIB”](#) na stránce 23

Rozšířený transakční klient používá parametry TPM a AXLIB k vyhledání funkcí ax_reg a ax_unreg správce transakcí. Tyto funkce se používají pouze v případě, že správce front používá dynamickou registraci.

[“Zotavení po selhání v rozšířeném transakčním zpracování”](#) na stránce 24

Po selhání musí být správce transakcí schopen obnovit všechny nekompletní jednotky práce. Aby to bylo možné provést, správce transakcí musí být schopen otevřít správce front správce front, který se účastnil nedokončené transakce v době selhání.

Aspekty produktu IBM WebSphere MQ for z/OS pro rozšířená připojení transakčních klientů

Někteří správci transakcí XA používají posloupnosti koordinačních volání transakcí, které jsou nekompatibilní s funkcemi běžně dostupnými pro klienty připojující se k produktu IBM WebSphere MQ for z/OS.

Je-li zjištěna nekompatibilní posloupnost, může produkt IBM WebSphere MQ for z/OS pro připojení vydat nestandardní konec a vrátit chybovou odezvu na klienta.

Například, xa_prepare přijme Abend 5C6-00D4007D, s návratovým kódem -3 (XAER_RMERR) vráceným klientovi.

Pro správce transakcí, kteří se setkají s touto situací, proveďte následující akce, které umožní správci transakcí interakci s produktem IBM WebSphere MQ for z/OS:

- Použijte opravu pro APAR PI49236.
- Povolte změnu poskytovanou serverem PI49236 pro kanál připojení serveru používaný správcem transakcí.

Změnu povolíte zadáním klíčového slova CSQSERVICE1 (v případě velkých písmen) kdekoli v poli popisu kanálu SVRCONN.

Všimněte si, že kanály s klíčovým slovem CSQSERVICE1 mají následující omezení:

- Dispozice GROUP odebrání zotavení není povolena. Povolena je pouze dispozice QMGR obnovy zotavení. Volání xa_open uvádějící název skupiny sdílení front v parametru **xa_info** selhává s parametrem *xaer_inval*.
- Volby MQGMO_LOCK a MQGMO_UNLOCK nejsou povoleny. Volání MQGET s parametrem MQGMO_LOCK nebo MQGMO_UNLOCK selže s chybou MQRC_ENVIRONMENT_ERROR.

Související pojmy

“Konfigurace správců transakcí s podporou standardu XA” na stránce 19

Nejprve nakonfigurujte základního klienta produktu IBM MQ a potom nakonfigurujte rozšířenou transakční funkci s použitím informací v těchto tématech.

Formát řetězce xa_open

Řetězec xa_open obsahuje dvojice definovaných názvů parametrů a hodnot.

Řetězec xa_open má následující formát:

```
parm_name1 = parm_value1, parm_name2 = parm_value2, ...
```

kde *parm_name* je název parametru a *parm_value* je hodnota parametru. Názvy parametrů nejsou citlivé na velikost písmen, ale pokud není uvedeno jinak, jsou hodnoty parametrů citlivé na velikost písmen. Parametry můžete zadat v libovolném pořadí.

Názvy, významy a platné hodnoty parametrů jsou následující:

Název

Význam a platné hodnoty

CHANNEL

Název kanálu MQI.

Jedná se o volitelný parametr. Je-li tento parametr zadán, musí být zadán také parametr CONNAME.

TRPTYPE

Komunikační protokol pro kanál MQI. Zde jsou platné hodnoty:

LU62

LU technologie SNA 6.2

NETBIOS

NetBIOS

SPX

IPX/SPX

TCP

Protokol TCP/IP

Jedná se o volitelný parametr. Pokud je vynechán, předpokládá se předvolená hodnota TCP. Hodnoty tohoto parametru nejsou citlivé na velikost písmen.

CONNAME

Síťová adresa správce front na serverovém konci kanálu MQI. Platné hodnoty tohoto parametru závisí na hodnotě parametru TRPTYPE:

LU62

Symbolický název místa určení, který identifikuje položku informací o připojení CPI-C.

Kvalifikovaný název partnerské LU sítě není platnou hodnotou, ani není alias partnerské LU. Důvodem je to, že zde nejsou žádné další parametry, které by určoval název transakčního programu (TP) a název režimu.

NETBIOS

Název NetBIOS .

SPX

4bajtová síťová adresa, 6bajtová adresa uzlu a volitelné dvoubajtové číslo soketu. Tyto hodnoty musí být uvedeny v hexadecimální notaci. Období musí oddělit adresy sítě a uzlu a číslo zásuvky, je-li dodáno, musí být uzavřeno v závorkách. Příklad:

```
0a0b0c0d.804abcde23a1(5e86)
```

Je-li číslo soketu vynecháno, předpokládá se výchozí hodnota 5e86 .

TCP

Název hostitele nebo adresa IP, volitelně následované číslem portu v závorkách. Je-li číslo portu vynecháno, předpokládá se výchozí hodnota 1414.

Jedná se o volitelný parametr. Je-li tento parametr zadán, musí být zadán také parametr CHANNEL.


QMNAME

Název správce front na straně serveru kanálu MQI. Název nesmí být prázdný ani obsahovat jednu hvězdičku (*), ani název nesmí začínat hvězdičkou. To znamená, že tento parametr musí identifikovat konkrétního správce front podle názvu.

Toto je povinný parametr.

Je-li klientská aplikace připojena ke specifickému správci front, musí být každá obnova transakce zpracována stejným správcem front.

Pokud se aplikace připojuje ke správci front produktu z/OS , pak může aplikace určit buď název specifického správce front, nebo název skupiny sdílení front (QSG). Při použití názvu správce front nebo názvu skupiny sdílení front aplikace řídí, zda bude v transakci pracovat s dispozicí QMGR obnovy nebo dispozicí SKUPINY zotavení. Skupina GROUP obnovy zotavení umožňuje, aby transakce byla zpracována na libovolném členu skupiny sdílení front. Chcete-li použít jednotky GROUP zotavení, musí být atribut správce front **GROUPUR** povolen.

 Další informace o použití jednotky zotavení skupiny GROUP najdete v tématu [Dispozice jednotky zotavení ve skupině sdílení front](#).

TPM

Správce transakcí, který se používá. Platné hodnoty jsou CICS a TUXEDO.

Rozšířený transakční klient používá tento parametr a parametr AXLIB pro stejný účel. Další informace o těchto parametrech naleznete v tématu [Parametry TPM a AXLIB](#).

Jedná se o volitelný parametr. Hodnoty tohoto parametru nejsou citlivé na velikost písmen.

SKLIB

Název knihovny, která obsahuje funkce ax_reg a ax_unreg správce transakcí.

Jedná se o volitelný parametr.

Identifikátor UID

ID uživatele, které je poskytnuto pro správce front k ověření. Je-li tento parametr zadán, musí být zadán také parametr **PWD** . Je-li zadané ID uživatele a heslo ověřeno, ID uživatele se použije pro identifikaci připojení správce transakcí s čísly. ID uživatele a heslo naplní objekt MQCSP na volání MQCONN.

Parametry **UID** a **PWD** jsou platné pro vazby klienta i serveru.

PWD

Heslo, které je poskytnuto správci front za účelem ověření. Je-li tento parametr zadán, musí být zadán také parametr **UID** .

Varování: V některých případech se heslo ve struktuře MQCSP pro klientskou aplikaci odešle přes síť jako prostý text. Chcete-li zajistit, aby hesla klientských aplikací byla chráněna odpovídajícím způsobem, prohlédněte si téma [Ochrana heslem produktu IBM MQCSP](#).

Zde je příklad řetězce xa_open:

```
channel=MARS.SVR, trptype=tcp, conname=MARS(1415), qmname=MARS, tpm=cics
```


Parametry CHANNEL, TRPTYPE, CONNAME a QMNAME řetězce xa_open


Tyto informace vám pomohou pochopit, jak rozšířený transakční klient používá tyto parametry k určení správce front, k němuž se má připojit.

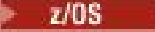
Jsou-li v řetězci xa_open zadány parametry CHANNEL a CONNAME, používá rozšířený transakční klient tyto parametry a parametr TRPTYPE pro spuštění kanálu MQI pro správce front serveru.

Nejsou-li parametry CHANNEL a CONNAME zadány v řetězci xa_open, rozšířený transakční klient používá hodnotu proměnné prostředí MQSERVER ke spuštění kanálu MQI. Není-li proměnná prostředí MQSERVER definována, použije rozšířený transakční klient položku v definici kanálu klienta identifikovanou parametrem QMNAME.

V každém z těchto případů rozšířený transakční klient kontroluje, zda hodnota parametru QMNAME odpovídá názvu správce front na serveru kanálu MQI. Pokud tomu tak není, volání xa_open se nezdaří a správce transakcí nahlásí selhání aplikace.

Pokud se aplikace připojuje ke správci front ve starší verzi než V7.0.1, volání xa_open bylo úspěšné, ale transakce má dispozice QMGR odebrání zotavení.  Ujistěte se, že aplikace, které vyžadují dispozice pro skupinu zotavení, se připojují pouze ke správcům front V7.0.1 nebo novější.

 Pokud aplikace používá název QSG v poli parametru QMNAME a vlastnost GROUPUR je zakázána ve správci front, k němuž se připojuje, volání xa_open selže.

 Pokud se klient aplikace připojuje ke správci front produktu z/OS verze V7.0.1 nebo novější, může pro parametr QMNAME zadat název skupiny sdílení front (QSG). To umožňuje aplikačnímu klientu podílet se na transakci se SKUPINOU transakcí dispozice zotavení. Další informace o jednotce SKUPINY zotavení naleznete v tématu [Dispozice jednotky zotavení](#).

Když klientská aplikace později volá volání MQCONN nebo MQCONNX ve stejném podprocesu, který správce transakcí použil k vydání volání xa_open, obdrží aplikace manipulátor připojení pro kanál MQI, který byl spuštěn voláním xa_open. Druhý kanál MQI není spuštěn. Rozšířený transakční klient kontroluje, zda je hodnota parametru *QMGrName* v rámci volání MQCONN nebo MQCONNX názvem správce front na konci kanálu MQI. Není-li tomu tak, volání MQCONN nebo MQCONNX selže s kódem příčiny MQRC_ANOTHER_Q_MGR_CONNECTED. Je-li hodnota parametru *QMGrName* prázdná nebo jedna hvězdička (*) nebo začíná se hvězdičkou, volání MQCONN nebo MQCONNX selže s kódem příčiny MQRC_Q_MGR_NAME_ERROR.

Pokud klientská aplikace již spustila kanál MQI voláním MQCONN nebo MQCONNX, než správce transakcí zavolá řetězec xa_open ve stejném podprocesu, správce transakcí místo toho použije tento kanál MQI. Druhý kanál MQI není spuštěn. Rozšířený transakční klient kontroluje, zda je hodnota parametru QMNAME v řetězci xa_open název správce front serveru. Pokud tomu tak není, volání xa_open selhává.

Pokud aplikace klienta nejprve spustí kanál MQI, může být hodnota parametru *QMGrName* v rámci volání MQCONN nebo MQCONNX prázdná nebo může obsahovat jednu hvězdičku (*), nebo může začínat hvězdičkou. Za těchto okolností je však nutné zajistit, aby správce front, ke kterému se aplikace připojuje, byl stejný jako správce front, který má správce transakcí otevřít jako správce prostředků, když později volá řetězec xa_open ve stejném podprocesu. Pokud tedy hodnota parametru *QMGrName* identifikuje správce front explicitně podle názvu, můžete se setkat s méně problémy.

Parametry TPM a AXLIB

Rozšířený transakční klient používá parametry TPM a AXLIB k vyhledání funkcí ax_reg a ax_unreg správce transakcí. Tyto funkce se používají pouze v případě, že správce front používá dynamickou registraci.

Je-li parametr TPM zadán v řetězci xa_open, ale parametr AXLIB není zadán, rozšířený transakční klient předpokládá hodnotu parametru AXLIB na základě hodnoty parametru TPM. Viz [Tabulka 4 na stránce 24](#), kde jsou převzaty hodnoty parametru AXLIB.

Tabulka 4. Předpokládané hodnoty parametru AXLIB

Hodnota produktu TPM	Platforma	Předpokládaná hodnota AXLIB
CICS	AIX	/usr/lpp/encina/lib/libEncServer.a(EncServer_shr.o)
CICS	HP-UX	/opt/encina/lib/libEncServer.sl
CICS	Solaris	/opt/encina/lib/libEncServer.so
CICS	Systémy Windows	Server libEnc
Tuxedo	AIX	/usr/lpp/tuxedo/lib/libtux.a(libtux.so.60)
Tuxedo	HP-UX	/opt/tuxedo/lib/libtux.sl
Tuxedo	Solaris	/opt/tuxedo/lib/libtux.so.60
Tuxedo	Systémy Windows	libtux

Je-li parametr AXLIB zadán v řetězci xa_open, rozšířený transakční klient používá svou hodnotu k přepsání jakékoli předpokládané hodnoty založené na hodnotě parametru TPM. Parametr AXLIB může být také použit pro správce transakcí, pro který parametr TPM nemá uvedenou hodnotu.

Další zpracování chyb pro xa_open

Volání xa_open selhává za určitých okolností.

Témata v tomto oddílu popisují situace, ve kterých volání xa_open selhává. Také selže, pokud se vyskytne některá z následujících situací:

- V řetězci xa_open došlo k chybě.
- Pro spuštění kanálu MQI nejsou k dispozici dostatečné informace.
- Vyskytl se problém při pokusu o spuštění kanálu MQI (například správce front serveru není spuštěn).

Zotavení po selhání v rozšířeném transakčního zpracování

Po selhání musí být správce transakcí schopen obnovit všechny nekompletní jednotky práce. Aby to bylo možné provést, správce transakcí musí být schopen otevřít správce front správce front, který se účastnil nedokončené transakce v době selhání.

Proto musíte zajistit, aby všechny nedokončené jednotky práce byly vyřešeny před provedením změn jakýchkoli konfiguračních informací.

Alternativně se musíte ujistit, že změny konfigurace nemají vliv na schopnost správce transakcí otevřít správce front, který potřebuje otevřít. Zde jsou uvedeny příklady takových změn konfigurace:

- Změna obsahu řetězce xa_open
- Změna hodnoty proměnné prostředí MQSERVER
- Změna položek v tabulce definic kanálů klienta (CCDT)
- Odstranění definice kanálu připojení serveru

Struktury přepínačů XA

S rozšířeným transakčním klientem na každé platformě jsou dodávány dvě struktury přepínačů XA.

Tyto struktury přepínačů jsou:

MQRMIXASwitch

Tuto strukturu přepínačů používá správce transakcí v případě, že správce front, který vystupuje jako správce prostředků, nepoužívá dynamickou registraci.

MQRMIXASwitchDynamic

Tuto strukturu přepínačů používá správce transakcí v případě, že správce front, který vystupuje jako správce prostředků, používá dynamickou registraci.

Tyto struktury přepínačů jsou umístěny v knihovnách, které jsou zobrazeny v [Tabulka 5](#) na stránce 25.

<i>Tabulka 5. Knihovny IBM MQ obsahující struktury přepínačů XA</i>	
Platforma	Knihovna obsahující struktury přepínačů XA
AIX HP-UX Linux Solaris	<code>MQ_INSTALLATION_PATH/lib/libmqcxa</code>
Systémy Windows	<code>MQ_INSTALLATION_PATH\bin\mqcxa.dll</code> ¹

`MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ.

Název správce prostředků IBM MQ v každé struktuře přepínače je `MQSeries_XA_RMI`, ale mnoho správců front může sdílet stejnou strukturu přepínačů.

Související pojmy

“Dynamická registrace a rozšířené transakční zpracování” na stránce 25

Použití dynamické registrace je formou optimalizace, protože může snížit počet volání funkce `xa_` vydaných správcem transakcí.

Dynamická registrace a rozšířené transakční zpracování

Použití dynamické registrace je formou optimalizace, protože může snížit počet volání funkce `xa_` vydaných správcem transakcí.

Pokud správce front nepoužívá dynamickou registraci, správce transakcí zapojí správce front do každé jednotky práce. Správce transakcí provede toto volání řetězcem `xa_start`, `xa_end` a `xa_prepare`, a to i v případě, že správce front nemá v rámci pracovní jednotky žádné prostředky, které by byly aktualizovány.

Pokud správce front používá dynamickou registraci, spustí se správce transakcí za předpokladu, že správce front není zapojen do pracovní jednotky, a nevolá řetězec `xa_start`. Správce front se poté zapojí do jednotky práce pouze tehdy, jsou-li její prostředky aktualizovány v rámci ovládacího prvku synchronizačního bodu. Pokud k tomu dojde, rozšířený transakční klient volá `ax_reg`, aby zaregistroval zapojení správce front.

Použití rozšířeného transakčního klienta s kanály SSL

Pomocí řetězce `xa_open` nelze nastavit kanál SSL. Postupujte podle těchto pokynů, chcete-li použít tabulku definic kanálů klienta (`ccdt`).

Informace o této úloze

Vzhledem k omezené velikosti řetězce `xa_open` `xa_info` není možné předávat všechny informace nezbytné k nastavení kanálu SSL při použití metody `xa_open` string pro připojení ke správci front. Proto musíte buď použít tabulku definic kanálů klienta, nebo, pokud to správce transakcí umožňuje, vytvořit kanál s `MQCONN` před vyvoláním volání `xa_open`.

Chcete-li použít tabulku definic kanálů klienta, proveďte následující kroky:

Postup

1. Určete řetězec `xa_open` obsahující pouze povinný parametr `qmname` (název správce front), například:
`XA_Open_String=qmname=MYQM`
2. Pomocí správce front definujte kanál `CLNTCONN` (client-connection) s požadovanými parametry zabezpečení SSL. Zahrňte název správce front do atributu `QMNAME` v definici `CLNTCONN`. Tato hodnota se bude shodovat s názvem `qmname` v řetězci `xa_open`.
3. Zpřístupněte definici `CLNTCONN` pro klientský systém v tabulce definic kanálů klienta (`CCDT`) nebo v Windowsv aktivním adresáři.

4. Používáte-li tabulku CCDT, identifikujte tabulku CCDT obsahující definici kanálu CLNTCONN s použitím proměnných prostředí MQCHLLIB a MQCHLTAB. Nastavte tyto proměnné v prostředí, které používá aplikace klienta i správce transakcí.

Výsledky

To dává správci transakcí definici kanálu pro příslušného správce front s atributy SSL potřebnými pro správné ověření, včetně hodnoty SSLCIPH, CipherSpec.

Konfigurace rozšířeného transakčního klienta pro produkt CICS

Rozšířený transakční klient pro použití produktem CICS můžete nakonfigurovat přidáním definice prostředku XAD do oblasti CICS .

Přidejte definici prostředku XAD pomocí online definice prostředku CICS (RDO), **cicsadd**. Definice prostředku XAD uvádí následující informace:

- Řetězec xa_open
- Úplný název cesty k souboru načtení přepínače

One switch load file is supplied for use by CICS on each of the following platforms: AIX, HP-UX, Solaris, and Windows systems. Každý soubor pro načtení přepínače obsahuje funkci, která vrací ukazatel na strukturu přepínačů XA, která se používá pro dynamickou registraci, MQRMIXASwitchDynamic. Úplný název cesty pro každý zaváděcí soubor přepínače viz [Tabulka 6](#) na stránce 26 .

Tabulka 6. Soubory načtení přepínače	
Platforma	Zaváděcí soubor přepínače
AIX HP-UX Linux Solaris	MQ_INSTALLATION_PATH/lib/amqczsc
Systémy Windows	MQ_INSTALLATION_PATH\bin\mqcc4swi.dll ¹

MQ_INSTALLATION_PATH představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

Zde je příklad definice prostředku XAD pro systémy Windows :

```
cicsadd -c xad -r REGION1 WMQXA \
  ResourceDescription="IBM MQ queue manager MARS" \
  XAOpen="channel=MARS.SVR, trptype=tcp, connname=MARS(1415), qmname=MARS, tpm=cics" \
  SwitchLoadFile="C:\Program Files\IBM\WebSphere MQ\bin\mqcc4swi.dll"
```

Další informace o přidání definice prostředku XAD do regionu CICS naleznete v příručce *CICS Administration Reference* a v příručce *CICS Administration Guide* pro vaši platformu.

Všimněte si následujících informací o použití produktu CICS s rozšířeným transakčním klientem:

- Do oblasti CICS lze přidat pouze jednu definici prostředku XAD pro IBM MQ . To znamená, že k oblasti může být přidružen pouze jeden správce front a všechny aplikace produktu CICS spuštěné v regionu se mohou připojit pouze k tomuto správci front. Chcete-li spustit aplikace produktu CICS , které se připojují k jinému správci front, je třeba spustit aplikace v jiném regionu.
- Každý aplikační server v regionu volá řetězec xa_open při inicializaci a spouští kanál MQI pro správce front přidruženého k oblasti. To znamená, že správce front musí být spuštěn před spuštěním aplikačního serveru, jinak se volání xa_open nezdaří. Všechny aplikace produktu IBM MQ MQI client později zpracované aplikačním serverem používají stejný kanál MQI.
- Je-li spuštěn kanál MQI a na straně klienta kanálu neexistuje žádná uživatelská procedura zabezpečení, je ID uživatele, které přechází z klientského systému do agenta MCA připojení k serveru, cics. Za

určitých okolností správce front použije toto ID uživatele pro kontrolu oprávnění, když se agent MCA připojení následně pokusí o přístup k prostředkům správce front v zastoupení klientské aplikace. Je-li toto ID uživatele použito pro kontrolu oprávnění, musíte se ujistit, že má oprávnění pro přístup ke všem prostředkům, které potřebuje k přístupu.

Informace o tom, kdy správce front používá toto ID uživatele pro kontroly oprávnění, najdete v tématu [Zabezpečení](#).

- Uživatelské procedury ukončení úlohy CICS , které jsou dodávány pro použití v klientských systémech IBM MQ , jsou uvedeny v seznamu [Tabulka 7 na stránce 27](#). Tyto uživatelské procedury nakonfigurujete stejným způsobem, jako jste nakonfigurovali odpovídající uživatelské procedury pro systémy serveru IBM MQ . Pro tyto informace se proto podívejte na téma [Povolení uživatelských procedur CICS](#).

<i>Tabulka 7. Ukončení ukončení úlohy CICS</i>		
Platforma	Zdroj	Knihovna
AIX HP-UX Linux Solaris	amqzscgx.c	amqzscg
Systémy Windows	amqzscgn.c	mqcc1415.dll

Konfigurace rozšířeného transakčního klienta pro Tuxedo

Chcete-li nakonfigurovat definici prostředku XAD pro použití produktem Tuxedo, aktualizujte soubor UBBCONFIG a tabulku správce prostředků.

Chcete-li nakonfigurovat definici prostředku XAD pro použití produktem Tuxedo, proveďte následující akce:

- V sekci GROUPS v souboru UBBCONFIG produktu Tuxedo pro aplikaci použijte parametr OPENINFO k určení řetězce xa_open.

Příklad toho, jak to provést, najdete v ukázkovém souboru UBBCONFIG, který je dodáván pro použití s ukázkovými programy produktu Tuxedo. V systémech AIX, HP-UX a Solaris je název souboru ubbstxc.cfg a v systému Windows je název souboru ubbstxcn.cfg.

- V položce pro správce front v tabulce správce prostředků produktu Tuxedo:
 - udataobj/RM (AIX, HP-UX a Solaris)
 - udataobj\rm (systémy Windows)

Určete název struktury přepínače XA a úplný název cesty ke knihovně, která obsahuje strukturu. Příklad toho, jak to lze provést pro jednotlivé platformy, najdete v tématu [Ukázky TUXEDO](#). Produkt Tuxedo podporuje dynamickou registraci správce prostředků, a proto můžete použít buď MQRMIXASwitch, nebo MQRMIXASwitchDynamic.

Microsoft Transakční server

Před tím, než můžete použít MTS jako správce transakcí, není třeba žádná další konfigurace. Existují však body, které je třeba poznamenat.

Všimněte si následujících informací o použití MTS s rozšířeným transakčním klientem:

- Aplikace MTS vždy při připojení ke správci front serveru spouští kanál MQI. MTS, ve své roli správce transakcí, používá ke komunikaci se správcem front stejný kanál MQI.
- Po selhání musí být MTS schopen obnovit všechny nedokončené jednotky práce. K tomu musí být MTS schopen komunikovat s libovolným správcem front, který se účastnil nedokončené jednotky práce v době selhání.

Když se aplikace MTS připojí ke správci front serveru a spustí kanál MQI, rozšířený transakční klient extrahuje dostatečné informace z parametrů volání MQCONN nebo MQCONNX, aby umožnil opětovné spuštění kanálu po selhání, pokud je to požadováno. Rozšířený transakční klient předává informace do MTS a MTS zaznamenává informace do svého protokolu.

Pokud aplikace MTS vydá volání MQCONN, tyto informace jsou jednoduše názvem správce front. Pokud aplikace MTS vydá volání MQCONNX a poskytuje strukturu definice kanálu MQCD, obsahuje informace také název kanálu MQI, síťovou adresu správce front serveru a komunikační protokol pro kanál.

V situaci zotavení MTS předává tyto informace zpět rozšířenému transakčnímu klientovi a rozšířený transakční klient jej používá k restartování kanálu MQI.

Pokud budete někdy potřebovat změnit informace o konfiguraci, ujistěte se, že všechny nedokončené jednotky práce byly vyřešeny před provedením změn. Alternativně se ujistěte, že změny konfigurace nemají vliv na schopnost rozšířeného transakčního klienta restartovat kanál MQI pomocí informací zaznamenaných serverem MTS. Zde jsou uvedeny příklady takových změn konfigurace:

- Změna hodnoty proměnné prostředí MQSERVER
- Změna položek v tabulce definic kanálů klienta (CCDT)
- Odstranění definice kanálu připojení serveru
- Všimněte si následujících podmínek, když používáte rozšířeného transakčního klienta s MTS:
 - V rámci jednoho podprocesu může být klientská aplikace připojena pouze k jednomu správci front v daném okamžiku.
 - Každý podproces aplikace klienta se může připojit k jinému správci front.
 - Klientská aplikace nemůže používat sdílené obslužné rutiny připojení.

Definování kanálů MQI

Chcete-li vytvořit nový kanál, musíte vytvořit **dvě** definice kanálu, jeden pro každý konec připojení, a to pomocí stejného názvu kanálu a kompatibilních typů kanálů. V tomto případě jsou typy kanálů *server-připojení* a *připojení klienta*.

Kanály definované uživatelem

Pokud server automaticky nedefinuje kanály, existují dva způsoby vytvoření definic kanálů a poskytnutí aplikace IBM MQ na počítači s přístupem počítače IBM MQ MQI client ke kanálu.

Tyto dvě metody jsou podrobně popsány:

1. Vytvořte jednu definici kanálu na klientu produktu IBM MQ a na druhé straně na serveru.

Toto platí pro libovolnou kombinaci IBM MQ MQI client a platformou serverů. Použijte jej, když začínal pracovat na systému, nebo testovat nastavení.

Podrobné informace o způsobu použití této metody naleznete v příručce [“Vytváření připojení k serveru a připojení klienta na různých platformách”](#) na stránce 34 .

2. Vytvořte obě definice kanálů na počítači serveru.

Tuto metodu použijte v případě, že nastavujete více kanálů a IBM MQ MQI client počítačů současně.

Podrobné informace o způsobu použití této metody naleznete v příručce [“Vytvoření připojení k serveru a připojení klienta na serveru”](#) na stránce 37 .

Automaticky definované kanály

Produkty IBM MQ na platformách jiných než z/OS zahrnují funkci, která může automaticky vytvořit definici kanálu na serveru, pokud taková neexistuje.

Je-li požadavek na připojení typu Inbound obdržen od klienta a nelze v daném správci front nalézt odpovídající definici připojení k serveru, produkt IBM MQ ji automaticky vytvoří a přidá do správce front. Automatická definice je založena na definici výchozího kanálu připojení serveru SYSTEM.AUTO.SVRCONN. Automatickou definici definic připojení serveru můžete povolit aktualizací objektu správce front pomocí

příkazu ALTER QMGR s parametrem CHAD (nebo pomocí příkazu PCF Change Queue Manager s parametrem ChannelAutoDef).

Související pojmy

“Řídící funkce kanálů” na stránce 152

Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

Windows

Linux

UNIX

Vytvoření a použití kanálů AMQP

Když instalujete podporu produktu IBM MQ pro rozhraní API MQ Light do instalace produktu IBM MQ , můžete spuštěním příkazů IBM MQ MQSC (**runmqsc**) definovat, změnit, odstranit, spustit a zastavit kanál. Můžete také zobrazit stav kanálu.

Než začnete

Tato úloha předpokládá, že jste nainstalovali kanál AMQP. Tuto akci provedete výběrem komponenty služby AMQP při instalaci produktu IBM MQ. Chcete-li získat další informace, použijte odkaz na vaši platformu a vyhledejte řádek tabulky "AMQP Service":

- **AIX** [Komponenty produktu IBM MQ pro systémy AIX](#)
- **HP-UX** [Komponenty produktu IBM MQ pro systémy HP-UX](#)
- **Linux** [Komponenty IBM MQ rpm pro systémy Linux](#)
- **Solaris** [Komponenty produktu IBM MQ pro systémy Solaris](#)
- **Windows** [Funkce produktu IBM MQ pro systémy Windows](#)

Chcete-li vytvořit testovací připojení ke správci front, musíte mít klienta MQ Light . Klienti produktu MQ Light jsou k dispozici pro produkt Node.js, Ruby, Java™ a Python. Další informace o dostupných klientech naleznete na webu komunity [IBM MQ Light](#).

Tato úloha je založena na klientovi MQ Light Node.js . Kroky vztahující se ke správci front produktu IBM MQ jsou však stejné pro všechny klienty.

Informace o této úloze

Následující procedura předpokládá, že máte existující neprodukční správce front, upgradovaný na úroveň příkazu 801. Chcete-li povolit servisní úroveň 801 pro správce front, můžete spustit následující příkaz:

```
stimqm -e CMDLEVEL=801 <QMNAME>
```

Po spuštění tohoto příkazu je třeba restartovat správce front. Pokud vyžadujete nového správce front, je zahrnut ukázkový skript umístěný v adresáři `<mqinstall>/amqp/samples` . Skript vytvoří nového správce front na úrovni příkazů 801, spustí službu AMQP, vytvoří nový kanál s názvem SAMPLE.AMQP.CHANNEL a spustí kanál. Pokud spustíte vzorový skript, buď `SampleMQM.sh` na Linux, nebo `SampleMQM.bat` v systému Windows, můžete spustit následující proceduru v kroku 6.

Poznámka: Kanály AMQP nepodporují uživatelem definované služby AMQP. Kanály AMQP podporují pouze výchozí nastavení systému SYSTEM.AMQP.SERVICE .

Pokud převedete existujícího správce front na úroveň příkazů 801, bude vytvořen nový výchozí objekt kanálu. Výchozí kanál se nazývá SYSTEM.DEF.AMQP. Můžete použít výchozí kanál k testování připojení produktu MQ Light ke správci front nebo můžete vytvořit nový kanál.

Následující procedura používá výchozí kanál.

Postup

1. Spusťte **runmqsc** z adresáře `<mqinstall>/bin/` :

```
runmqsc <QMNAME>
```

2. Zkontrolujte, zda je funkce AMQP nainstalována a funguje správně.

Použijte příkaz **START SERVICE** ke spuštění služby IBM MQ , která řídí prostředí JVM:

```
START SERVICE(SYSTEM.AMQP.SERVICE)
```

3. Nastavte ID uživatele MCAUSER .

Pokud se klient AMQP připojí ke kanálu, kanál určuje ID uživatele MCAUSER , které se používá pro připojení ke správci front. Výchozí hodnota MCAUSER je prázdná. Před připojením jakýchkoli klientů AMQP ke správci front je třeba určit hodnotu parametru MCAUSER , která musí být platným uživatelem produktu IBM MQ , který je autorizován k publikování a odběru témat IBM MQ .

- a) Pomocí příkazu **ALTER CHANNEL** nastavte ID uživatele MCAUSER :

```
ALTER CHANNEL(SYSTEM.DEF.AMQP) CHLTYPE(AMQP) MCAUSER(Useř ID)
```

- b) Pomocí následujících dvou příkazů produktu **setmqaut** můžete autorizovat své ID uživatele MCAUSER pro publikování a odběr témat:

```
setmqaut -m <QMNAME> -t topic -n SYSTEM.BASE.TOPIC -p <MCAUSER>  
-all +pub +sub
```

a

```
setmqaut -m <QMNAME> -t qmgr -p <MCAUSER> -all +connect
```

Pokud je kanál spuštěn během přidání nebo změny ID uživatele MCAUSER , je třeba kanál zastavit a znovu spustit.

Poznámka: Pokud není nastaveno ID uživatele MCAUSER nebo ID uživatele MCAUSER nemá autorizaci pro publikování nebo přihlášení k odběru témat IBM MQ , obdržíte v klientovi AMQP chybovou zprávu.

4. Použijte příkaz **START CHANNEL** ke spuštění výchozího SYSTEM.DEF.AMQP :

```
START CHANNEL(SYSTEM.DEF.AMQP)
```

5. Chcete-li zkontrolovat stav kanálu, použijte příkaz **DISPLAY CHSTATUS** :

```
DISPLAY CHSTATUS(SYSTEM.DEF.AMQP) CHLTYPE(AMQP)
```

Je-li kanál spuštěn správně, zobrazí se ve výstupu příkazu hodnota STATUS(RUNNING) .

6. Změňte výchozí port.

Výchozí port pro připojení AMQP 1.0 je 5672. Pokud již používáte port 5672, což je možné, pokud jste již dříve nainstalovali produkt MQ Light, je třeba změnit port používaný kanálem AMQP. Pro změnu portu použijte příkaz **ALTER CHANNEL** :

```
ALTER CHANNEL(SYSTEM.DEF.AMQP) CHLTYPE(AMQP) PORT(NEW PORT NUMBER)
```

7. Nechcete-li blokovat nebo filtrovat připojení k kanálu AMQP pomocí pravidel ověřování kanálu (CHLAUTH), zakažte ověření kanálu ve správci front následujícím způsobem:

```
alter qmgr chlauth(disabled)
```

Nedoporučuje se zakázat ověřování připojení ve správci produkčních front. Ověřování připojení byste měli zakázat pouze ve vývojovém prostředí.

Můžete také konfigurovat pravidla ověřování kanálu správce front tak, aby povolovala specifická připojení k kanálu AMQP.

8. Volitelné: Chcete-li povolit šifrování protokolu SSL/TLS v kanálu s použitím konfigurovaného úložiště klíčů pro správce front, je třeba nastavit atribut SSLCIPH pro příslušný kanál na příslušnou specifikaci šifry. Ve výchozím nastavení je specifikace šifry prázdná, což znamená, že šifrování SSL/TLS není na kanálu použito. Chcete-li nastavit specifikaci šifry, použijte příkaz **ALTER CHANNEL**. Příklad:

```
ALTER CHANNEL(SYSTEM.DEF.AMQP) CHLTYPE(AMQP) SSLCIPH(CIPHER SPECIFICATION)
```

Kromě toho existuje řada dalších voleb konfigurace kanálu přidružených k šifrování SSL/TLS, které lze nastavit takto:

- Při výchozím nastavení je certifikát v úložišti klíčů správce front s popisem, který odpovídá atributu CERTLABL správce front, použit jako název používaný šifrováním SSL/TLS pro daný kanál. Můžete vybrat jiný certifikát nastavením CERTLABL. Použijte příkaz **ALTER CHANNEL** k uvedení návěští pro požadovaný certifikát:

```
ALTER CHANNEL(SYSTEM.DEF.AMQP) CHLTYPE(AMQP) CERTLABL(CERTIFICATE LABEL)
```

- Můžete nastavit kanál tak, aby byl vyžadován certifikát z připojení klienta SSL/TLS. Můžete vybrat, zda se od připojení klienta SSL/TLS požaduje certifikát nastavením SSLCAUTH. Příkaz **ALTER CHANNEL** se používá k nastavení, zda je požadován certifikát od připojení klienta SSL/TLS. Příklad:

```
ALTER CHANNEL(SYSTEM.DEF.AMQP) CHLTYPE(AMQP) SSLCAUTH(REQUIRED or OPTIONAL)
```

- **V 8.0.0.15** Nastavíte-li atribut SSLCAUTH na hodnotu REQUIRED, bude možné zkontrolovat rozlišující název (DN) certifikátu od klienta. Chcete-li zkontrolovat rozlišující název certifikátu z klienta, nastavte atribut SSLPEER. Chcete-li zkontrolovat rozlišující název certifikátu od klienta, použijte příkaz **ALTER CHANNEL**. Příklad:

```
ALTER CHANNEL(SYSTEM.DEF.AMQP) CHLTYPE(AMQP) SSLPEER (DN SPECIFICATION)
```

Případně můžete také použít záznamy ověření kanálu k povolení nebo blokování připojení, protože tato metoda nabízí větší granularitu ve srovnání s použitím atributu SSLPEER. Další informace o nastavení parametru SSLPEER a o použití záznamů ověření kanálu jako alternativy najdete v tématu [SSL Peer](#).

9. Nainstalujte klienta MQ Light Node.js spuštěním následujícího příkazu:

```
npm install mqlight
```

10. Přejděte do adresáře `node_modules/mqlight/samples` a spusťte ukázkovou aplikaci příjemce:

- Používáte-li výchozí číslo portu, můžete spustit ukázkovou aplikaci příjemce:

```
node recv.js
```

- Pokud jste nakonfigurovali kanál AMQP tak, aby používal jiné číslo portu, můžete vzorovou aplikaci příjemce spustit s parametrem a zadat nové číslo portu:

```
node recv.js -s amqp://localhost:6789
```

Při úspěšném připojení k výchozímu kanálu se zobrazí následující zpráva:

```
Connected to amqp://localhost:5672 using client-id recv_e79c55d
Subscribed to pattern: public
```

Aplikace je nyní připojena ke správci front a čeká na příjem zpráv. Je přihlášen k odběru tématu `public`.

Poznámka: The `client-id` is automatically generated, unless you specify one using the `-i` parameter.

11. V novém okně příkazového řádku přejděte do adresáře `node_modules/mqlight/samples` a spusťte ukázkovou aplikaci odesílatele spuštěním následujícího příkazu:

```
node send.js
```

V okně s příkazovým řádkem aplikace příjemce se zobrazí zpráva `Ahoj světe`.

12. Chcete-li obdržet ukázkovou zprávu MQ Light, použijte ukázkou **AMQSSUB** IBM MQ.

V systémech Linux a Windows lze ukázkou nalézt v následujících umístěních:

- **Linux** `mqinstall/samp/bin` v systému Linux.
- **Windows** `mqinstall/Tools\c\Samples\Bin` v systému Windows.

- a) Spusťte ukázkou spuštěním následujícího příkazu:

```
amqssub public <QM-name>.
```

- b) Odešlete zprávu do aplikace IBM MQ opětovným spuštěním následujícího příkazu:

```
node send.js
```

13. Chcete-li vytvořit více kanálů AMQP, použijte příkaz **DEFINE CHANNEL** :

```
DEFINE CHANNEL(MY.AMQP.CHANNEL) CHLTYPE(AMQP) PORT(2345)
```

Definujete-li kanál, je třeba jej spustit ručně pomocí příkazu **START CHANNEL** :

```
START CHANNEL(MY.AMQP.CHANNEL)
```

Chcete-li zkontrolovat, zda je kanál spuštěn správně, můžete spustit ukázkovou aplikaci příjemce s určením portu nového kanálu:

```
node recv.js -s amqp://localhost:2345
```

Jak pokračovat dále

Chcete-li zobrazit připojení produktu IBM MQ, zastavit kanál a odstranit kanál, můžete použít následující příkazy:

DISPLAY CONN(*) TYPE(CONN) WHERE (CHANNEL EQ SYSTEM.DEF.AMQP)

Zobrazí připojení produktu IBM MQ, které kanál AMQP provedl ve správci front.

DISPLAY CHSTATUS(*) CHLTYPE(AMQP) CLIENTID(*) ALL

Zobrazí seznam klientů AMQP připojených k uvedenému kanálu.

STOP CHANNEL (MY.AMQP.CHANNEL)

Zastaví kanál AMQP a zavře port, na kterém naslouchá.

DELETE CHANNEL (MY.AMQP.CHANNEL)

Odstraní všechny kanály, které jste vytvořili.

Poznámka: Neodstraňujte výchozí kanál `SYSTEM.DEF.AMQP`.

Můžete určit, zda je schopnost AMQP nainstalována do instalace produktu IBM MQ a zda je k ní přidružen správce front, a to pomocí produktu **runmqsc** nebo **PCF**:

- Pomocí produktu **runmqsc** zobrazte atributy správce front a zkontrolujte, zda je k dispozici příkaz AMQPCAP (YES).
- Pomocí příkazu PCF použijte příkaz **MQCMD_INQUIRE_Q_MGR** a potvrďte hodnotu parametru MQIA_AMQP_CAPABILITY.

Související informace

[strmqm](#)

[Vyvíjení klientských aplikací AMQP](#)

[Zabezpečení klientů AMQP](#)

Windows

Linux

UNIX

Odebrání kanálu AMQP ze správců front

Kanál AMQP lze odebrat ze správců front odebráním složek z instalačního adresáře.

Postup

1. Zastavte správce front.
2. Odeberte podporu produktu IBM MQ pro rozhraní API MQ Light:

- **AIX** V produktu AIX spusťte následující příkaz:

```
installp -u mqm.amqp.rte
```

- **Linux** V systému Linux odeberte balík RPM AMQP. Pokud jste balík RPM znovu zabalili před jeho instalací, zadejte název znovu zabaleného balíku RPM.

```
rpm -e MQSeriesAMQP
```

- **Windows** V systému Windows odeberte složku amqp z instalace produktu IBM MQ. Ujistěte se, že v instalační cestě produktu IBM MQ nejsou odebrány žádné další soubory nebo složky.

3. Restartujte správce front.

Související informace

[Vyvíjení klientských aplikací AMQP](#)

[Zabezpečení klientů AMQP](#)

Windows

Linux

UNIX

Soubory protokolu kanálu AMQP

Soubory protokolu pro kanály AMQP jsou uloženy ve stejném datovém adresáři produktu IBM MQ jako soubory protokolu produktu IBM MQ.

Výchozí datový adresář na Windows je C:\ProgramData\IBM\MQ.

Výchozí datový adresář na Linux je /var/mqm.

Kanál AMQP zapisuje informace z protokolů do následujících souborů protokolů, které se nacházejí v datovém adresáři produktu IBM MQ:

- amqp.stdout, zapsána do složky qmgrs/<QM-name>.
- amqp.stderr, zapsána do složky qmgrs/<QM-name>.
- amqp_*.log, zapsána do složky qmgrs/<QM-name>/errors.

Pokud klient MQ Light obdrží chybu ověření nebo autorizace, může vám administrátor vyhledat podrobné informace o příčině selhání zabezpečení v souboru amqp_0.log a v souborech MQ_AMQERR*.log.

Všechny soubory FDC se vytvářejí jako soubory AMQP*.FDC, které se zapisují do složky <data-directory>/errors.

Některé konfigurační soubory se zapisují do adresáře `qmgrs/<QM-name>/amqp` . V tomto adresáři není třeba upravovat žádné soubory.

Související informace

[Chybové protokoly v systému SYSTÉM UNIX, Linuxa Okna](#)



[Vyvíjení klientských aplikací AMQP](#)

[Zabezpečení klientů AMQP](#)

Vytváření připojení k serveru a připojení klienta na různých platformách

Můžete vytvořit každou definici kanálu na počítači, na který se vztahuje. Existují omezení, jak můžete vytvářet definice kanálů na klientském počítači.

Na všech platformách můžete pomocí příkazů skriptu IBM MQ Script (MQSC), příkazů PCF (Programmable command Format) nebo Průzkumníka IBM MQ definovat kanál připojení serveru na serverovém počítači.

 V systému z/OS můžete také použít panely Operace a Ovládací panely. 
V systému IBM i můžete také použít rozhraní panelu.

Vzhledem k tomu, že příkazy MQSC nejsou k dispozici na počítači, kde byl produkt IBM MQ nainstalován pouze jako produkt IBM MQ MQI client , musíte v počítači klienta používat různé způsoby definování kanálu připojení klienta.

Použití produktu `runmqsc`

Můžete zadat parametr `-c` a volitelně parametr `-u` pro připojení `runmqsc` jako klienta ke správci front, kterého chcete spravovat.

Použijete-li parametr `-u` k zadání ID uživatele, budete vyzváni k zadání odpovídajícího hesla.

Pokud jste záznam `CONNAUTH AUTHINFO` nakonfigurovali s `CHCKLOCL (REQUIRED)` nebo `CHCKLOCL (REQDADM)` , musíte použít parametr `-u` , jinak nebudete schopni spravovat správce front s `runmqsc` .

Související pojmy

[“Vytvoření kanálu připojení klienta na serveru IBM MQ MQI client” na stránce 35](#)

Na pracovní stanici klienta můžete definovat kanál připojení klienta pomocí `MQSERVER` nebo pomocí struktury `MQCNO` na volání `MQCONN` .

Související úlohy

[“Definování kanálu připojení serveru na serveru” na stránce 34](#)

V případě potřeby spusťte prostředí MQSC a potom definujte kanál připojení serveru.

Definování kanálu připojení serveru na serveru

V případě potřeby spusťte prostředí MQSC a potom definujte kanál připojení serveru.

Postup

1. Volitelné: Pokud vaše platforma serveru není z/OS, nejprve vytvořte a spusťte správce front a poté spusťte příkazy MQSC.
 - a) Vytvořte správce front s názvem `QM1` , například:

```
ctmqm QM1
```

- b) Spusťte správce front:

```
stmqm QM1
```

- c) Spusťte příkazy MQSC:

```
runmqsc QM1
```

2. Definujte kanál s vybraným názvem a typem kanálu *server-connection*.

```
DEFINE CHANNEL(CHAN1) CHLTYPE(SVRCONN) TRPTYPE(TCP) +  
DESCR('Server-connection to Client_1')
```

Tato definice kanálu je přidružena ke správci front spuštěnému na serveru.

3. Pomocí následujícího příkazu můžete povolit přístup pro příchozí připojení k vašemu správci front:

```
SET CHLAUTH(CHAN1) TYPE(ADDRESSMAP) ADDRESS('IP address') MCAUSER('userid')
```

- Kde SET CHLAUTH používá název kanálu definovaného v předchozím kroku.
- Kde 'IP adresa' je adresa IP klienta.
- Kde 'userid' je ID, které chcete poskytnout kanálu pro řízení přístupu k cílovým frontám. V tomto poli se rozlišují velká a malá písmena.

Můžete zvolit identifikaci vašeho příchozího připojení pomocí několika různých atributů. Příklad používá adresu IP. Alternativní atributy zahrnují ID uživatele klienta a SSL nebo Rozlišovací jméno subjektu TLS. Další informace naleznete v tématu [Záznamy ověřování kanálu](#)

Vytvoření kanálu připojení klienta na serveru IBM MQ MQI client

Na pracovní stanici klienta můžete definovat kanál připojení klienta pomocí MQSERVER nebo pomocí struktury MQCNO na volání MQCONN.

Použití produktu MQSERVER

Proměnnou prostředí MQSERVER můžete použít k určení jednoduché definice kanálu připojení klienta. Je jednoduché v tom smyslu, že pomocí této metody můžete zadat pouze několik atributů kanálu.

- Určete jednoduchou definici kanálu na serveru Windows následujícím způsobem:

```
SET MQSERVER=ChannelName/TransportType/ConnectionName
```

- Určete jednoduchou definici kanálu v systémech SYSTÉM UNIX a Linux následujícím způsobem:

```
export MQSERVER=ChannelName/TransportType/ConnectionName
```

- Určete jednoduchou definici kanálu v systémech IBM i následujícím způsobem:

```
ADDENVVAR ENVVAR(MQSERVER) VALUE('ChannelName/TransportType/ConnectionName')
```

kde:

- ChannelName musí být stejný název, jaký je definován na serveru. Nesmí obsahovat dopředné lomítko.
- TransportType může být jedna z následujících hodnot, v závislosti na vaší platformě IBM MQ MQI client :
 - LU62
 - TCP
 - NETBIOS
 - SPX

Poznámka: Na systémech SYSTÉM UNIX a Linux je TransportType rozlišuje velikost písmen a musí být velkými písmeny. Volání MQCONN nebo MQCONNX vrátí hodnotu 2058, pokud není rozpoznán TransportType .

- ConnectionName je název serveru, jak je definován pro komunikační protokol (TransportType).

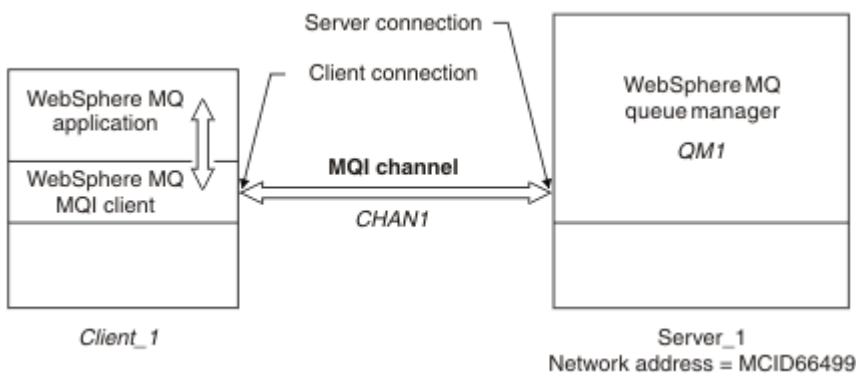
Například v systému Windows:

```
SET MQSERVER=CHANNEL1/TCP/MCID66499
```

nebo, v systémech SYSTÉM UNIX a Linux :

```
export MQSERVER=CHANNEL1/TCP/'MCID66499'
```

Poznámka: Informace o změně čísla portu TCP/IP naleznete v části [“SERVER MQSERVER”](#) na stránce 76.



Obrázek 1. Jednoduchá definice kanálu

Některé další příklady definic jednoduchého kanálu jsou:

- zapWindows:

```
SET MQSERVER=CHANNEL1/TCP/9.20.4.56
SET MQSERVER=CHANNEL1/NETBIOS/BOX643
```

- V systémech SYSTÉM UNIX a Linux:

```
export MQSERVER=CHANNEL1/TCP/'9.20.4.56'
export MQSERVER=CHANNEL1/LU62/BOX99
```

- **IBM i** zapIBM i:

```
ADDENVVAR ENVVAR(MQSERVER) VALUE('CHANNEL1/TCP/9.20.4.56(1416)')
```

kde BOX99 je LU 6.2 ConnectionName.

Na serveru IBM MQ MQI clientse všechny požadavky **MQCONN** nebo **MQCONNX** pokusí použít kanál, který jste definovali, pokud není kanál přepsán ve struktuře MQCD, na kterou odkazuje struktura MQCNO zadaná pro produkt **MQCONNX**.

Poznámka: Další informace o proměnné prostředí **MQSERVER** viz [“SERVER MQSERVER”](#) na stránce 76.

Použití struktury MQCNO u volání MQCONNX

Aplikace produktu IBM MQ MQI client může použít strukturu voleb připojení MQCNO u volání produktu **MQCONNX** pro odkazování na strukturu definice kanálu MQCD, která obsahuje definici kanálu připojení klienta.

Tímto způsobem může klientská aplikace určit atributy **ChannelName**, **TransportType** a **ConnectionName** kanálu za běhu programu a umožnit tak připojení klientské aplikace k více správcům front serveru současně.

Všimněte si, že pokud definujete kanál pomocí proměnné prostředí *MQSERVER*, není možné určit za běhu atributy **ChannelName**, **TransportType** a **ConnectionName**.

Klientská aplikace může také určovat atributy kanálu, jako je například **MaxMsgLength** a **SecurityExit**. Zadání těchto atributů umožňuje aplikaci klienta určit hodnoty pro atributy, které nejsou výchozími hodnotami, a umožňuje volání ukončovacích programů kanálu na straně klienta kanálu MQI.


Pokud kanál používá zabezpečení SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security), může klientská aplikace také poskytovat informace související se zabezpečením SSL nebo TLS ve struktuře MQCD. Další informace související s SSL nebo TLS mohou být poskytnuty ve struktuře voleb konfigurace SSL nebo TLS, MQSCO, který je také odkazován strukturou MQCNO na volání **MQCONN**.


Další informace o strukturách MQCNO, MQCD a MQSCO naleznete v části [MQCNO](#), [MQCD](#) a [MQSCO](#).

Poznámka: Ukázkový program pro MQCONN se nazývá **amqscnxc**. Jiný ukázkový program s názvem **amqsslc** demonstruje použití struktury MQSCO.

Vytvoření připojení k serveru a připojení klienta na serveru

Na serveru můžete vytvořit obě definice a potom zpřístupnit definici klienta-připojení klientovi.

Nejprve definujte kanál připojení serveru a poté definujte kanál připojení klienta. Na všech platformách můžete pomocí příkazů skriptu IBM MQ Script (MQSC), příkazů programu PCF (Programmable command Format) nebo Průzkumníka IBM MQ definovat kanál připojení serveru na počítači serveru. 

V systému z/OS můžete také použít panely Operace a Ovládací panely.  V systému IBM i můžete také použít rozhraní panelu.

Definice kanálu připojení klienta vytvořené na serveru jsou k dispozici klientům s použitím tabulky CCDT (Client Channel Definition table).

Související pojmy

[“Tabulka definic kanálů klienta” na stránce 37](#)

Tabulka definic kanálů klienta (CCDT) určuje definice kanálu a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformách jiných než z/OS je tabulka CCDT vytvořena automaticky. Poté jej musíte zpřístupnit klientské aplikaci.

Související úlohy

[“Definování kanálu připojení serveru na serveru” na stránce 40](#)

Vytvořte definici kanálu připojení serveru pro daného správce front.

[“Definování kanálu pro připojení klienta na serveru” na stránce 40](#)

Při definování kanálu připojení serveru je nyní definován příslušný kanál připojení klienta.

[“Přístup k definicím kanálu připojení klienta” na stránce 41](#)

Zpřístupněte tabulku CCDT (Client Channel Definition table) klientským aplikacím zkopírováním nebo sdílením, poté zadejte jeho umístění a název na klientském počítači.

Tabulka definic kanálů klienta

Tabulka definic kanálů klienta (CCDT) určuje definice kanálu a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformách jiných než z/OS je tabulka CCDT vytvořena automaticky. Poté jej musíte zpřístupnit klientské aplikaci.

Účelem tabulky CCDT (Client Channel Definition table) je určit definice kanálu používané klientskými aplikacemi pro připojení ke správci front. Definice kanálu také určuje ověřovací informace, které platí pro připojení.

CCDT je binární soubor. Je generován správcem front. Správce front nechte soubor CCDT.

Na jiných platformách než z/OS je tabulka CCDT vytvořena při vytvoření správce front. Kanály připojení klienta se přidávají do tabulky, když použijete příkaz **DEFINE CHANNEL** a jejich definice se změní, když zadáte příkaz **ALTER CHANNEL**.

Notes:

- Návrh souboru CCDT produktu IBM MQ je takový, že soubor CCDT je zmenšen, pouze po skutečném definování všech kanálů připojení klienta definovaných uživatelem. Je-li kanál připojení klienta odstraněn, je v souboru CCDT označen jako odstraněný, ale není fyzicky odebrán.
- Chcete-li vynutit zmenšení souboru tabulky CCDT po odstranění jednoho nebo více kanálů připojení klienta, zadejte následující příkaz:

```
rcimqobj -m QM80 -t clchltab
```

Pomocí tabulky CCDT můžete klientům poskytnout informace o ověření, abyste mohli zkontrolovat odvolání certifikátů SSL. Definujte seznam názvů obsahující objekty ověřovacích informací a nastavte atribut správce front **SSLCRLNameList** tak, aby obsahoval název seznamu názvů.

Existuje řada způsobů, jak aplikaci klienta použít tabulku CCDT. Nástroje CCDT lze kopírovat na klientský počítač. CCDT můžete zkopírovat do umístění sdíleného více než jedním klientem. Nástroje CCDT lze zpřístupnit klientovi jako sdílený soubor, zatímco zůstává umístěn na serveru.

Pokud používáte FTP ke zkopírování souboru, použijte volbu **bin** k nastavení binárního režimu; nepoužívejte výchozí režim **ASCII**. Bez ohledu na to, zda chcete zpřístupnit tabulky CCDT, musí být umístění zabezpečeno, aby se zabránilo neoprávněným změnám kanálů.

Jiné platformy serveru než z/OS

Výchozí tabulky CCDT s názvem **AMQCLCHL.TAB** se vytvářejí při vytváření správce front.

Ve výchozím nastavení **AMQCLCHL.TAB** je umístěn v následujícím adresáři na serveru:

- **IBM i** V systému IBM i v integrovaném systému souborů:

```
/QIBM/UserData/mqm/qmgrs/QUEEMANAGERNAME/&ipcc
```

- **Linux** **UNIX** V systémech SYSTÉM UNIX a Linux:

```
/prefix/qmgrs/QUEEMANAGERNAME/@ipcc
```

Název adresáře, na který se odkazuje **QUEEMANAGERNAME**, je na systémech SYSTÉM UNIX a Linux rozlišen rozlišováním malých a velkých písmen. Název adresáře se nemusí shodovat s názvem správce front, je-li v něm uveden speciální znaky názvu správce front.

- **Windows** zapWindows:

```
MQ_INSTALLATION_PATH\data\qmgrs\QUEEMANAGERNAME\@ipcc
```

MQ_INSTALLATION_PATH představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ.

Možná jste však zvolili použití jiného adresáře pro data správce front. Při použití příkazu **crtmqm** můžete zadat parametr **-md DataPath**. Pokud ano, **AMQCLCHL.TAB** se nachází v adresáři **@ipcc DataPath**, kterou jste zadali.

Cestu k tabulce CCDT lze změnit nastavením **MQCHLLIB**. Pokud jste nastavili **MQCHLLIB**, mějte na paměti, že pokud máte více správců front na stejném serveru, budou sdílet stejné umístění CCDT.

CCDT se vytvoří při vytvoření správce front. Každá položka tabulky CCDT představuje připojení klienta ke specifickému správci front. Nový záznam se přidá, když definujete kanál připojení klienta pomocí příkazu

DEFINE CHANNEL , a položka se aktualizuje, když pozměníte kanály připojení klienta pomocí příkazu **ALTER CHANNEL** .

Klientské platformy na serveru IBM MQ 8.0

CCDT můžete na klientském počítači vytvořit přímo pomocí příkazu `runmqsc` s parametrem **-n** . CCDT se vytvoří v umístění indikovaném parametrem `MQCHLLIB` a s názvem souboru, který je označen jako `MQCHLTAB` , což je standardně `AMQCLCHL.TAB` .

Všimněte si, že pokud zadáte argument **-n** , nesmíte uvést žádný jiný parametr.

Každá položka tabulky CCDT představuje připojení klienta ke specifickému správci front. Nový záznam se přidá, když definujete kanál připojení klienta pomocí příkazu **DEFINE CHANNEL** , a položka se aktualizuje, když pozměníte kanály připojení klienta pomocí příkazu **ALTER CHANNEL** .

Jak specifikovat umístění tabulky CCDT na klientovi

V systému klienta můžete určit umístění tabulky CCDT dvěma způsoby:

- Pomocí proměnných prostředí `MQCHLLIB` určete adresář, kde se tabulka nachází, a `MQCHLTAB` , abyste uvedli název souboru tabulky.
- Použijte se konfigurační soubor klienta. Ve stanze `CHANNELS` použijte atributy `ChannelDefinitionDirectory` k uvedení adresáře, kde je tabulka umístěna, a `ChannelDefinitionFile` pro uvedení názvu souboru.

Je-li umístění určeno v konfiguračním souboru klienta i pomocí proměnných prostředí, proměnné prostředí budou mít prioritu. Tuto funkci můžete použít k určení standardního umístění v konfiguračním souboru klienta a k přepsání pomocí proměnných prostředí, je-li to nutné.

Související odkazy

[“MQCHLLIB” na stránce 73](#)

`MQCHLLIB` uvádí cestu k adresáři se souborem obsahujícím tabulku definic kanálů klienta (CCDT). Soubor je vytvořen na serveru, ale lze jej zkopírovat na pracovní stanici IBM MQ MQI client .

Související informace

[Práce se zrušenými certifikáty](#)

Migrace a tabulky definic kanálů klienta (CCDT)

Obecně lze říci, že interní formát tabulky definic kanálů klienta se může měnit z jedné úrovně vydání IBM MQ na další. V důsledku toho může produkt IBM MQ MQI client použít tabulku definic kanálů klienta pouze v případě, že je připraven správcem front serveru, který má stejnou úroveň vydání jako klient, nebo na dřívější úrovni vydání.

Verze 7.1 IBM MQ MQI client může použít tabulku definic kanálů klienta, která byla připravena správcem front Verze 6.0 . Klient produktu Verze 6.0 však nemůže použít tabulku definic kanálů klienta, která byla připravena správcem front Verze 7.1 .

Kanály připojení klienta v Active Directory

Na systémech Windows , které podporují Active Directory, IBM MQ publikuje kanály připojení klienta v Active Directory , aby poskytl dynamickou vazbu klient-server.

Jsou-li definovány objekty kanálu připojení klienta, jsou zapsány do souboru soubor definice kanálu klienta s názvem `AMQCLCHL.TAB` při výchozím nastavení. Pokud kanály připojení klienta používají protokol TCP/IP, publikuje je server IBM MQ také v adresáři Active Directory. Když klient IBM MQ určí, jak se připojit k serveru, hledá odpovídající definici objektu kanálu připojení klienta pomocí následujícího pořadí vyhledávání:

1. Datová struktura `MQCONN` `MQCD`
2. proměnná prostředí `MQSERVER`
3. definiční soubor kanálu klienta

4. Active Directory

Toto pořadí znamená, že žádné aktuální aplikace nebudou ovlivněny žádnou změnou. Tyto záznamy v Active Directory si můžete představit jako záznamy v souboru definic kanálů klienta a klient IBM MQ je zpracovává stejným způsobem. Chcete-li nakonfigurovat a spravovat podporu pro publikování definic kanálů připojení klienta v Active Directory, použijte příkaz `setmqscp`, jak je popsáno v souboru `setmqscp`.

Definování kanálu připojení serveru na serveru

Vytvořte definici kanálu připojení serveru pro daného správce front.

Postup

1. Na počítači serveru definujte kanál s vámi zvoleným názvem a typem kanálu *server-connection*.
Příklad:

```
DEFINE CHANNEL(CHAN2) CHLTYPE(SVRCONN) TRPTYPE(TCP) +  
DESCR('Server-connection to Client_2')
```

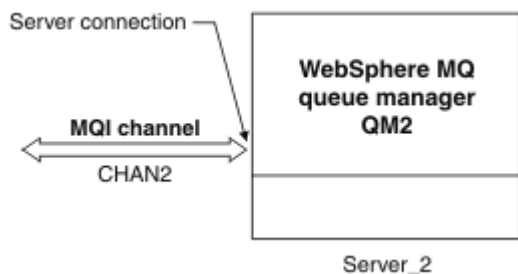
2. Pomocí následujícího příkazu můžete povolit přístup pro příchozí připojení k vašemu správci front:

```
SET CHLAUTH(CHAN2) TYPE(ADDRESSMAP) ADDRESS('IP address') MCAUSER('userid')
```

- Kde SET CHLAUTH používá název kanálu definovaného v předchozím kroku.
- Kde 'IP adresa' IP adresa je adresa IP klienta.
- Kde 'userid' je ID, které chcete poskytnout kanálu pro řízení přístupu k cílovým frontám. V tomto poli se rozlišují velká a malá písmena.

Můžete zvolit identifikaci vašeho příchozího připojení pomocí několika různých atributů. Příklad používá adresu IP. Alternativní atributy zahrnují ID uživatele klienta a SSL nebo Rozlišovací jméno subjektu TLS. Další informace naleznete v tématu [Záznamy ověřování kanálu](#)

Tato definice kanálu je přidružena ke správci front spuštěnému na serveru.



Obrázek 2. Definování kanálu připojení serveru

Definování kanálu pro připojení klienta na serveru

Při definování kanálu připojení serveru je nyní definován příslušný kanál připojení klienta.

Než začnete

Definujte kanál připojení serveru.

Postup

1. Definujte kanál se stejným názvem jako kanál připojení serveru, ale typ kanálu *klient-připojení*. Je třeba uvést název připojení (CONNNAME). Pro TCP/IP je název připojení síťová adresa nebo název hostitele počítače serveru. Je také vhodné zadat název správce front (QMNAME), do kterého má být vaše aplikace IBM MQ spuštěna v klientském prostředí, aby se mohla připojit. Změnou názvu správce front můžete definovat sadu kanálů pro připojení k různým správcům front.


```
DEFINE CHANNEL(CHAN2) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNNAME(9.20.4.26) QMNAME(QM2) DESCR('Client-connection to Server_2')
```

2. Pomocí následujícího příkazu můžete povolit přístup pro příchozí připojení k vašemu správci front:

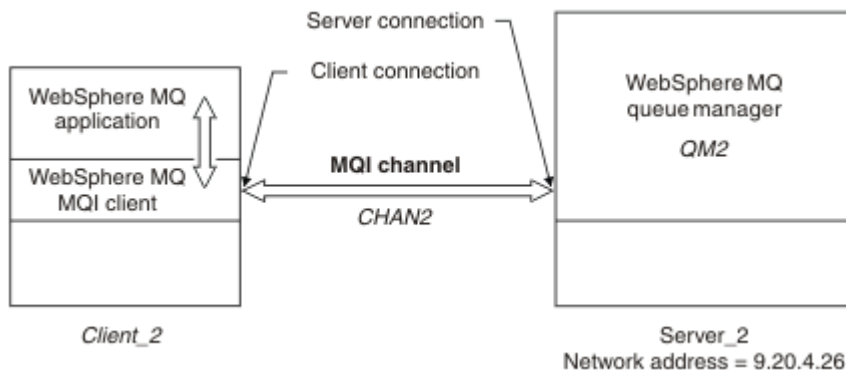
```
SET CHLAUTH(CHAN2) TYPE(ADDRESSMAP) ADDRESS('IP-adresa') MCAUSER('userid')
```

- Kde SET CHLAUTH používá název kanálu definovaného v předchozím kroku.
- Kde 'IP adresa' je adresa IP klienta.
- Kde 'userid' je ID, které chcete poskytnout kanálu pro řízení přístupu k cílovým frontám. V tomto poli se rozlišují velká a malá písmena.

Můžete zvolit identifikaci vašeho příchozího připojení pomocí několika různých atributů. Příklad používá adresu IP. Alternativní atributy zahrnují ID uživatele klienta a SSL nebo Rozlišovací jméno subjektu TLS. Další informace naleznete v tématu [Záznamy ověřování kanálu](#)

Výsledky

Na jiných platformách než z/OSse tato definice kanálu ukládá do souboru s názvem tabulky CCDT (Client Channel Definition table), který je přidružen ke správci front. Tabulka definic kanálů klienta může obsahovat více než jednu definici kanálu připojení klienta. Další informace o tabulce definic kanálů klienta a o příslušných informacích o tom, jak jsou definice kanálů připojení klienta k dispozici v produktu z/OS, viz ["Tabulka definic kanálů klienta"](#) na stránce 37.



Obrázek 3. Definování kanálu připojení klienta

Přístup k definicím kanálu připojení klienta

Zpřístupněte tabulku CCDT (Client Channel Definition table) klientským aplikacím zkopírováním nebo sdílením, poté zadejte jeho umístění a název na klientském počítači.

Než začnete

Definovali jste kanály připojení klienta, které potřebujete.

V systému z/OSjste vytvořili tabulku CCDT. Na ostatních platformách je tabulka CCDT automaticky vytvořena a aktualizována.

Informace o této úloze

Aby aplikace klienta používala tabulku definic kanálů klienta (CCDT), musíte zpřístupnit tabulky CCDT a zadat její umístění a název.

Postup

1. Zpřístupněte tabulky CCDT klientským aplikacím jedním ze tří způsobů:

- a) Volitelné: Zkopírujte tabulky CCDT na klientský počítač.
- b) Volitelné: Zkopírujte tabulku CCDT do umístění sdíleného více než jedním klientem.
- c) Volitelné: Opustit CCDT na serveru, ale umožnit jeho sdílení klientem.

Bez ohledu na umístění, které jste vybrali pro tabulky CCDT, musí být umístění zabezpečeno, aby se zabránilo neautorizovaným změnám kanálů.

2. Na straně klienta zadejte umístění a název souboru obsahujícího tabulky CCDT jedním ze tří způsobů:

- a) Volitelné: Použijte sekci CHANNELS konfiguračního souboru klienta. Další informace viz [“stanza CHANNELS konfiguračního souboru klienta”](#) na stránce 59.
- b) Volitelné: Použijte proměnné prostředí MQCHLLIB a MQCHLTAB.

Proměnné prostředí můžete nastavit například zadáním příkazu:

- V systémech HP Integrity NonStop Servera SYSTÉM UNIX a Linux :

```
export MQCHLLIB= MQ_INSTALLATION_PATH/qmgrs/ QUEUEMANAGERNAME /@ipcc
export MQCHLTAB=AMQCLCHL.TAB
```

-  zapIBM i:

```
ADDENVVAR ENVVAR(MQCHLLIB) VALUE('/QIBM/UserData/mqm/qmgrs/QUEUEMANAGERNAME/@ipcc')
ADDENVVAR ENVVAR(MQCHLTAB) VALUE(AMQCLCHL.TAB)
```

kde *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

- c) Volitelné: Pouze v systému Windows použijte řídicí příkaz produktu **setmqscp** k publikování definic kanálů připojení klienta v Active Directory .

Je-li nastavena proměnná prostředí MQSERVER, klient IBM MQ používá definici kanálu připojení klienta určenou parametrem MQSERVER jako předvolbu pro všechny definice v tabulce definic kanálů klienta.

Programy pro ukončení kanálů pro kanály MQI

Pro prostředí IBM MQ MQI client v systémech UNIX, Linux a Windows jsou k dispozici tři typy ukončení kanálu.

Patří mezi ně:

- Ukončení odeslání
- Ukončení příjmu
- Uživatelská procedura pro zabezpečení zprávy

Tyto uživatelské procedury jsou dostupné jak na straně klienta, tak na straně serveru kanálu. Pokud používáte proměnnou prostředí MQSERVER, nejsou uživatelské procedury k dispozici pro vaši aplikaci. Uživatelské procedury kanálu jsou vysvětleny v tématu [Programy výstupních programů kanálů pro kanály systému zpráv](#).

Uživatelské procedury send a receive spolupracují. Existuje několik možných způsobů, jak je použít:

- Rozdělení a opětovné přiřazení zprávy
- Komprese a dekomprimace dat ve zprávě (tato funkce je poskytována jako součást produktu IBM MQ, ale možná budete chtít použít jinou kompresní techniku)
- šifrování a dešifrování uživatelských dat (tato funkčnost je poskytována jako součást produktu IBM MQ, ale možná budete chtít použít jinou techniku šifrování)
- Žurnalování každé odeslané a přijaté zprávy

Ukončení zabezpečení můžete použít k zajištění správného určení klienta a serveru IBM MQ a k řízení přístupu.

Je-li na straně připojení serveru k instanci kanálu odesílání nebo příjem instance kanálu nutné provést volání MQI v rámci připojení, ke kterému jsou přidruženy, použijte manipulátor připojení, který je uveden v poli MQCXP Hconn . Musíte si být vědomi toho, že operace odeslání a přijetí klienta s připojením nemůže provádět volání MQI.

Související pojmy

[“Zabezpečení se ukončí na připojení klienta” na stránce 43](#)

Ukončovací programy zabezpečení můžete použít k ověření, že partner na druhém konci kanálu je pravý. Speciální pokyny platí, je-li pro připojení klienta použita uživatelská procedura pro zabezpečení zprávy.

Související odkazy

[“Cesta k východům” na stránce 43](#)

Výchozí cesta pro umístění uživatelských procedur kanálu je definována v konfiguračním souboru klienta. Uživatelské procedury kanálu jsou načteny při inicializaci kanálu.

[“Identifikace volání rozhraní API v ukončovacím programu pro odeslání nebo přijetí” na stránce 45](#)

Při použití kanálů MQI pro klienty určuje bajt 10 vyrovnávací paměti volání rozhraní API, které má být používáno při volání uživatelské procedury pro odeslání nebo příjem. To je užitečné k identifikaci toho, které toky kanálu obsahují uživatelská data a mohou vyžadovat zpracování, jako je šifrování nebo digitální podepisování.

Související informace

[Rozšíření zařízení správce front](#)

[Uživatelské procedury, uživatelské procedury rozhraní API a instalovatelné služby produktu IBM MQ](#)

Cesta k východům

Výchozí cesta pro umístění uživatelských procedur kanálu je definována v konfiguračním souboru klienta. Uživatelské procedury kanálu jsou načteny při inicializaci kanálu.

V systémech UNIX, Linux a Windows je při instalaci produktu IBM MQ MQI client do vašeho systému přidán konfigurační soubor klienta. Předvolená cesta pro umístění kanálů kanálu na klientovi je definovaná v tomto souboru, za použití stanzy:

```
ClientExitPath:  
ExitsDefaultPath= string  
ExitsDefaultPath64= string
```

kde *řetězec* je umístění souboru ve formátu vhodném pro platformu

Když je kanál inicializován po volání MQCONN nebo MQCONNX , prohledává se konfigurační soubor klienta. Stanza ClientExit je přečtena a všechny uživatelské procedury kanálu, které jsou určeny v definici kanálu, jsou načteny.

Zabezpečení se ukončí na připojení klienta

Ukončovací programy zabezpečení můžete použít k ověření, že partner na druhém konci kanálu je pravý. Speciální pokyny platí, je-li pro připojení klienta použita uživatelská procedura pro zabezpečení zprávy.

Obrázek 4 na stránce 45 ilustruje použití uživatelských procedur zabezpečení v připojení klienta pomocí správce oprávnění objektu IBM MQ k ověření uživatele. Ve struktuře MQCNO na straně klienta je ve struktuře MQCNO nastavena hodnota SecurityParmsPtr nebo SecurityParmsOffset a existují uživatelské procedury zabezpečení na obou koncích kanálu. Po dokončení běžné výměny zpráv zabezpečení a ke spuštění kanálu je struktura MQCSP přístupná z pole MQCXP SecurityParms předána do uživatelské procedury zabezpečení na straně klienta. Typ ukončení je nastaven na hodnotu MQXR_SEC_PARMS. Uživatelská procedura zabezpečení se může rozhodnout neprovádět nic pro identifikátor uživatele a heslo, nebo může změnit jednu nebo obě z nich. Data vrácená z uživatelské procedury se pak odešlou na konec kanálu na připojení serveru. Struktura MQCSP je znovu sestavena na konci kanálu připojení k serveru a je předána uživatelské proceduře zabezpečení připojení k serveru z pole MQCXP SecurityParms . Uživatelská procedura zabezpečení přijímá a zpracovává tato data. Toto zpracování obvykle provádí obrácení změn provedených v polích ID uživatele a hesla v uživatelské proceduře klienta, které se pak

používají k autorizaci připojení ke správci front. Výsledná struktura MQCSP se odkazuje pomocí parametru SecurityParmsPtr ve struktuře MQCNO v systému správce front.

Adresa paměti, která je předávána zpět polem MQCXP SecurityParms , musí zůstat adresovatelná a nezměněná, dokud nebude MQXR_TERM. Uživatelská procedura nesmí zneplatnit nebo uvolnit paměť zpět systému před voláním procedury MQXR_TERM.

Pokud jsou parametry SecurityParmsPtr nebo SecurityParmsnastaveny ve struktuře MQCNO a dojde k ukončení zabezpečení pouze na jednom konci kanálu, přijme uživatelská procedura zabezpečení a zpracuje strukturu MQCSP. Akce jako šifrování jsou nevhodné pro jednu uživatelskou proceduru, protože neexistuje žádná uživatelská procedura pro provedení doplňkové akce.

Pokud nejsou parametry SecurityParmsPtr a SecurityParmsnastaveny ve struktuře MQCNO a dojde k ukončení zabezpečení na obou koncích kanálu nebo na obou koncích kanálu, je volána procedura zabezpečení nebo uživatelské procedury zabezpečení. Ukončení zabezpečení může vrátit svou vlastní strukturu MQCSP adresovanou prostřednictvím Ptr SecurityParmsPtr. Uživatelská procedura zabezpečení se znovu nevolá, dokud nebude ukončena (ExitReason MQXR_TERM). Zapisovací program může uvolnit paměť používanou pro MQCSP v této fázi.

Když instance kanálu připojení serveru sdílí více než jednu konverzaci, je vzorec volání na proceduru zabezpečení omezen na druhou a následující konverzaci.

Při první konverzaci je vzor stejný, jako kdyby instance kanálu nesdíleli konverzace. Pro druhou a další konverzaci není uživatelská procedura zabezpečení nikdy volána s funkcí MQXR_INIT, MQXR_INIT_SEC nebo MQXR_SEC_MSG. Je volána s funkcí MQXR_SEC_PARMS.

V rámci instance kanálu se sdílením konverzací je MQXR_TERM volán pouze pro poslední spuštěnou konverzaci.

Každá konverzace má možnost v rámci volání MQXR_SEC_PARMS pro ukončení změnit objekt MQCD; na konci spojení mezi serverem a kanálem může být tato funkce užitečná například při změně hodnot MCAUserIdentifier nebo LongMCAUserIdPtr před provedením připojení ke správci front.

Server-connection exit	Client-connection exit
	Invoked with MQXR_INIT Responds with MQXCC_OK
Invoked with MQXR_INIT Responds with MQXCC_OK	
	Invoked with MQXR_INIT_SEC Responds with MQXCC_OK
Invoked with MQXR_INIT_SEC Responds with MQXCC_OK	
	Invoked with MQXR_SEC_PARMS Responds with MQXCC_OK
Invoked with MQXR_SEC_PARMS Responds with MQXCC_OK	
Data transfer begins	
Invoked with MQXR_TERM Responds with MQXCC_OK	Invoked with MQXR_TERM Responds with MQXCC_OK

Obrázek 4. Připojení klienta-iniciovaná výměna s dohodou pro připojení klienta pomocí parametrů zabezpečení

Poznámka: Aplikace uživatelské procedury zabezpečení vytvořené před vydáním produktu IBM MQ v7.1 mohou vyžadovat aktualizaci. Další informace najdete v tématu [Uživatelské programy zabezpečení kanálu](#).

Identifikace volání rozhraní API v ukončovacím programu pro odeslání nebo přijetí

Při použití kanálů MQI pro klienty určuje bajt 10 vyrovnávací paměti volání rozhraní API, které má být používáno při volání uživatelské procedury pro odesílání nebo příjem. To je užitečné k identifikaci toho, které toky kanálu obsahují uživatelská data a mohou vyžadovat zpracování, jako je šifrování nebo digitální podepisování.

Následující tabulka zobrazuje data, která se objevují v bajtu 10 kanálu toku při zpracování volání rozhraní API.

Poznámka: Tyto hodnoty nejsou jedinými hodnotami tohoto bajtu. Existují i další **rezervované** hodnoty.

Tabulka 8. Identifikace volání rozhraní API		
Volání rozhraní API	Hodnota bajtu 10 pro požadavek	Hodnota bajtu 10 pro odpověď
MQCONN "1" na stránce 46, "2" na stránce 46	X'81 '	X "91"
MQDISC "1" na stránce 46	X'82 '	X "92"

Tabulka 8. Identifikace volání rozhraní API (pokračování)

Volání rozhraní API	Hodnota bajtu 10 pro požadavek	Hodnota bajtu 10 pro odpověď
MQOPEN "3" na stránce 46	X'83 '	X "93"
MQCLOSE	X'84 '	X "94"
MQGET "4" na stránce 46	X'85 '	X "95"
MQPUT "4" na stránce 46	X'86 '	X "96"
Požadavek MQPUT1 "4" na stránce 46	X'87 '	X "97"
Požadavek MQSET	X'88 '	X "98"
Požadavek MQINQ	X'89 '	X "99"
Požadavek MQCMIT	X'8A'	X'9A'
Požadavek MQBACK	X'8B'	X'9B'
Požadavek MQSTAT	X'8D'	X'9D'
Požadavek MQSUB	X'8E'	X'9E'
Požadavek MQSUBRQ	X'8F'	X'9F'
Požadavek xa_start	X'A1'	X'B1'
požadavek xa_end	X'A2'	X'B2'
požadavek xa_open	X'A3'	X'B3'
požadavek xa_close	X'A4'	X'B4'
požadavek-xa_	X'A5'	X'B5'
Požadavek xa_commit	X'A6'	X'B6'
Požadavek xa_rollback	X'A7'	X'B7'
požadavek-xa_	X'A8'	X'B8'
Požadavek xa_rec	X'A9'	X'B9'
požadavek xa_complete	X'AA '	X'BA '

Notes:

1. Připojení mezi klientem a serverem je zahájeno klientskou aplikací pomocí MQCONN. Proto je pro tento příkaz zejména několik dalších toků sítě. To samé platí pro MQDISC, které ukončuje síťové připojení.
2. MQCONNX je pro účely připojení typu klient-server zpracován stejným způsobem jako MQCONN.
3. Je-li otevřen rozsáhlý distribuční seznam, může existovat více než jeden tok sítě na volání MQOPEN, aby byla předána všechna požadovaná data do kanálu SVRCONN MCA.
4. Velké zprávy mohou překročit velikost segmentu přenosu. Pokud k tomu dojde, může existovat mnoho síťových toků, které jsou výsledkem jediného volání rozhraní API.

z/OS Připojení klienta ke skupině sdílení front

Klienta lze připojit ke skupině sdílení front prostřednictvím vytvoření kanálu MQI mezi klientem a správcem front na serveru, který je členem skupiny sdílení front.

Skupina sdílení front je tvořena sadou správců front, kteří mají přístup ke stejné sadě sdílených front. Další informace o sdílených frontách naleznete v tématu [Sdílené fronty a skupiny sdílení front](#).

Klient, který se připojuje ke sdílené frontě, se může připojit ke všem členům skupiny sdílení front. Přínosy připojení ke skupině sdílení front jsou možné přírůstky front-endové a back-endové dostupnosti a zvýšení kapacity. Můžete se připojit ke specifickému správci front nebo ke generickému rozhraní.

Přímé připojení ke správci front ve skupině sdílení front poskytuje výhodu, kterou lze vkládat zprávy do sdílené cílové fronty, což zvyšuje dostupnost back-endového systému.

Při připojování ke generickému rozhraní skupiny sdílení front se otevře relace s jedním ze správců front ve skupině. To zvyšuje dostupnost front-endu, protože se správce front klienta může připojit k libovolnému správci front ve skupině. Připojte se ke skupině pomocí generického rozhraní, když se nechcete připojit ke specifickému správci front v rámci skupiny sdílení front.

Generické rozhraní může být distributorem Sysplex Distributor VIPA nebo generickým názvem prostředku VTAM nebo jiným společným rozhraním ke skupině sdílení front. Další informace o nastavení generického rozhraní naleznete v tématu [Nastavení komunikace pro produkt IBM MQ for z/OS pomocí skupin sdílení front](#).

Chcete-li se připojit ke generickému rozhraní skupiny sdílení front, je třeba vytvořit definice kanálu, ke kterým může správce front ve skupině přistupovat libovolný správce front. Chcete-li to provést, musíte mít stejné definice na každém správci front ve skupině.

Definujte kanál SVRCONN následujícím způsobem:

```
DEFINE CHANNEL(CHANNEL1) CHLTYPE(SVRCONN) TRPTYPE(TCP) +
QSGDISP(GROUP)
```

Definice kanálů na serveru jsou uloženy ve sdíleném úložišti produktu Db2. Každý správce front v rámci skupiny sdílení front vytvoří lokální kopii definice a zajistí, že se při zadání volání MQCONN nebo MQCONNX vždy připojíte ke správnému kanálu připojení serveru.

Definujte kanál CLNTCONN následujícím způsobem:

```
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNNAME( VIPA address ) QMNAME(QSG1) +
DESCR('Client-connection to Queue Sharing Group QSG1') QSGDISP(GROUP)
```

Protože je generické rozhraní skupiny sdílení front uloženo v poli CONNAME v kanálu připojení klienta, můžete se nyní připojit k libovolnému správci front v této skupině a zařadit do sdílených front vlastních touto skupinou.

Konfigurace klienta pomocí konfiguračního souboru

Nakonfigurujte své klienty pomocí atributů v textovém souboru. Tyto atributy mohou být přepsány proměnnými prostředí nebo jinými způsoby specifickými pro platformu.

Produkt IBM MQ MQI clients můžete nakonfigurovat pomocí textového souboru, konfiguračního souboru IBM MQ MQI client. Tento soubor je podobný konfiguračnímu souboru správce front `qm.ini`, který se používá v systémech SYSTÉM UNIX a Linux. Soubor obsahuje řadu oddílů, z nichž každý obsahuje řadu řádků ve formátu **attribute-name = hodnota**.

Konfigurační soubor IBM MQ MQI client je obecně pojmenován `mqclient.ini`, ale můžete mu dát jiný název. Informace o konfiguraci v tomto souboru platí pro všechny platformy a pro klienty, kteří používají rozhraní MQI, IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NET a XMS. Ačkoli se atributy v konfiguračním souboru IBM MQ MQI client vztahují na většinu klientů IBM MQ, existují některé atributy, které nejsou čteny spravovanými klienty .NET a XMS .NET nebo klienty, kteří používají buď IBM MQ classes for Java, nebo IBM MQ classes for JMS. Další informace viz [“Kteří klienti IBM MQ mohou číst každý atribut” na stránce 49](#).

Funkce konfigurace se vztahují na všechna připojení klientské aplikace ke všem správcům front, nikoli k jednotlivým připojením ke konkrétnímu připojení ke správci front. Atributy týkající se připojení k jednotlivým správcům front lze konfigurovat programově, například pomocí struktury MQCD, nebo pomocí tabulky CCDT (Client Channel Definition Table).

Proměnné prostředí, které byly podporovány ve verzích produktu IBM WebSphere MQ starších než Verze 7.0, jsou nadále podporovány a v případě, že se taková proměnná prostředí shoduje s ekvivalentní hodnotou v konfiguračním souboru klienta, proměnná prostředí přepíše hodnotu konfiguračního souboru klienta.

Pro klientskou aplikaci, která používá produkt IBM MQ classes for JMS, můžete také přepsat konfigurační soubor klienta následujícími způsoby:

- Nastavením vlastností v konfiguračním souboru JMS
- Nastavením systémových vlastností Java, které také potlačí konfigurační soubor JMS.

V případě klienta produktu .NET můžete také přepsat konfigurační soubor klienta a ekvivalentní proměnné prostředí pomocí konfiguračního souboru aplikace .NET.

Připojení více kanálů nelze nastavit pomocí konfiguračního souboru klienta.

Příklad konfiguračního souboru klienta

```
##* Module Name: mqclient.ini                                ##*
##* Type       : IBM MQ MQI client configuration file      ##*
##* Function   : Define the configuration of a client      ##*
##*                                                   ##*
##*****##
##* Notes     :                                           ##*
##* 1) This file defines the configuration of a client    ##*
##*                                                   ##*
##*****##

ClientExitPath:
  ExitsDefaultPath=/var/mqm/exits
  ExitsDefaultPath64=/var/mqm/exits64

TCP:
  Library1=DLLName1
  KeepAlive = Yes
  ClntSndBuffSize=32768
  ClntRcvBuffSize=32768
  Connect_Timeout=0

MessageBuffer:
  MaximumSize=-1
  Updatepercentage=-1
  PurgeTime=0

LU62:
  TPName
  Library1=DLLName1
  Library2=DLLName2

PreConnect:
  Module=amqldapi
  Function=myFunc
  Data=ldap://myLDAPServer.com:389/cn=wmq,ou=ibm,ou=com
  Sequence=1

CHANNELS:
  DefRecon=YES
  ServerConnectionParms=SALES.SVRCONN/TCP/hostname.x.com(1414)
```

Související odkazy

[“Použití proměnných prostředí IBM MQ” na stránce 71](#)

Tento oddíl popisuje proměnné prostředí, které lze použít s aplikacemi produktu IBM MQ MQI client.

[“Změna konfiguračních informací správce front” na stránce 105](#)

Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro IBM MQ.

Umístění konfiguračního souboru klienta

Konfigurační soubor IBM MQ MQI client se může nacházet v řadě lokalit.

Klientská aplikace používá následující vyhledávací cestu k vyhledání konfiguračního souboru IBM MQ MQI client :

1. Umístění zadané proměnnou prostředí MQCLNTCF.

Formát této proměnné prostředí je úplná adresa URL. To znamená, že název souboru nemusí být nutně mqclient.ini a usnadňuje umístění souboru v systému souborů připojeném k síti.

Všimněte si následujícího:

- Klienti produktů C, .NET a XMS podporují pouze protokol file: ; předpokládá se, že pokud řetězec adresy URL nezačíná řetězcem protocol: , bude použit protokol file: .
- Chcete-li povolit prostředí JRE produktu Java 1.4.2 , které nepodporují čtení proměnných prostředí, lze proměnnou prostředí MQCLNTCF potlačit pomocí systémové vlastnosti MQCLNTCF Java .

2. Soubor s názvem mqclient.ini v současném pracovním adresáři aplikace.

3. Soubor s názvem mqclient.ini v datovém adresáři IBM MQ pro systémy Windows, SYSTÉM UNIX a Linux .

Všimněte si následujícího:

- Datový adresář produktu IBM MQ neexistuje na určitých platformách, například IBM i a z/OS, nebo v případech, kdy byl klient dodán s jiným produktem.
- Na systémech SYSTÉM UNIX a Linux je to adresář /var/mqm .
- Na platformách Windows nakonfigurujte proměnnou prostředí MQ_DATA_PATH během instalace tak, aby ukazovala na datový adresář. Obvykle je C: \ProgramData\IBM\MQ

Poznámka: Instalujete-li pouze klienta, může být proměnná prostředí MQ_FILE_PATH.

- Chcete-li povolit prostředí JRE produktu Java 1.4.2 , která nepodporuje čtení proměnných prostředí, můžete proměnnou prostředí MQ_DATA_PATH ručně potlačit hodnotou proměnné prostředí MQ_DATA_PATH Java .

4. Soubor s názvem mqclient.ini ve standardním adresáři, který je vhodný pro platformu a je přístupný uživatelům:

- Pro všechny klienty produktu Java se jedná o hodnotu systémové vlastnosti user.home Java .
- Pro klienty jazyka C na platformách SYSTÉM UNIX a Linux se jedná o hodnotu proměnné prostředí HOME.
- Pro klienty jazyka C v systému Windows se jedná o zřetěžené hodnoty proměnných prostředí HOMEDRIVE a HOMEPATH.

Poznámka: V případě klienta IBM MQ pro HP Integrity NonStop Server musí být soubor mqclient.ini umístěn v systému souborů OSS. Aplikace Guardian musí buď umístit soubor mqclient.ini do datového adresáře IBM MQ , nebo nastavit proměnnou prostředí MQCLNTCF na umístění v systému souborů OSS.

Kteří klienti IBM MQ mohou číst každý atribut

Většina atributů v konfiguračním souboru IBM MQ MQI client může být použita klientem C a nespravovanými klienty .NET . Existují však některé atributy, které nejsou čteny spravovanými klienty .NET a XMS .NET nebo klienty, kteří používají buď IBM MQ classes for Java , nebo IBM MQ classes for JMS.

Tabulka 9. Které atributy se vztahují na každý typ klienta						
Název a atributy oddílu mqclient.ini	Popis	C a nespravováno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
stanza CHANNELS						

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravo váno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
<u>CCSID</u>	Kódované číslo znakové sady, které má být použito.	Ano	Ne	Ne	Ano	Ano
<u>ChannelDefinition</u>	Cesta k adresáři se souborem obsahujícím tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano
<u>ChannelDefinition</u>	Název souboru obsahujícího tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano
<u>ReconDelay</u>	Administrativní volba pro konfiguraci prodlevy opětného připojení pro klientské programy, které se mohou automaticky znovu připojit.	Ano	Ne	Ano	Ano	Ano

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravo váno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
<u>DefRecon</u>	Administrativní volba, která umožní klientským programům automaticky znovu navázat spojení nebo zakázat automatické opětovné připojení klientského programu, který byl napsán tak, aby se automaticky znovu připojil.	Ano	Ne	Ano	Ano	Ano
<u>MQReconnectTimeout</u>	Časový limit v sekundách, který se má znovu připojit ke klientovi.	Ano	Ne	Ne	Ano	Ne
<u>ParametryServerConnectionParms</u>	Umístění serveru IBM MQ a komunikační metoda, která má být použita.	Ano	Ne	Ne	Ano	Ano
<u>Put1DefaultAlwaysSync</u>	Řídí chování volání funkce MQPUT1 s volbou MQPMO_RESPONSE_AS_Q_DEF.	Ano	Ano	Ano	Ano	Ano

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravo váno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
PasswordProtection	Umožňuje nastavit chráněná hesla ve struktuře MQCSP raději než pomocí SSL nebo TLS.	Ano	Ano	Ano	Ano	Ano
ClientExit-stanza cesty						
ExitsDefaultPath	Určuje umístění 32bitového kanálu pro klienty.	Ano	Ano	Ano	Ano	Ano
ExitsDefaultPath64	Určuje umístění 64bitových kanálů kanálů pro klienty.	Ano	Ano	Ano	Ano	Ano
JavaExitsClassPath	Hodnoty, které mají být přidány do cesty ke třídě při spuštění uživatelské procedury produktu Java .	Ne	Ano	Ano	Ne	Ne
stanza JMQI						

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravo váno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
<u>useMQCSPAuthentication</u>	Řídí, zda aplikace IBM MQ classes for Java a IBM MQ classes for JMS mají při ověřování u správce front používat režim kompatibility nebo režim ověřování MQCSP.	Ne	Ano	Ano	Ne	Ne
stanzaMessageBuffer						
<u>MaximumSize</u>	Velikost vyrovnávací paměti dopředného čtení v kilobajtech, v rozsahu od 1 do 999 999.	Ano	Ano	Ano	Ano	Ano
<u>PurgeTime</u>	Interval, v sekundách, po jehož uplynutí jsou vyprázdněny zprávy ponechané ve vyrovnávací paměti dopředného čtení.	Ano	Ano	Ano	Ano	Ano

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravo váno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
<u>UpdatePercentage</u>	Hodnota aktualizace v procentech , v rozsahu 1-100, která se používá při výpočtu prahové hodnoty k určení toho, kdy klientská aplikace vytváří nový požadavek na server.	Ano	Ano	Ano	Ano	Ano
stanzaPreConnect						
<u>Data</u>	Adresa URL úložiště, kde jsou uloženy definice připojení.	Ano	Ne	Ne	Ne	Ne
<u>Funkce</u>	Název funkčního vstupního bodu do knihovny, která obsahuje výstupní kód PreConnect .	Ano	Ne	Ne	Ne	Ne
<u>Modul</u>	Název modulu obsahujícího kód ukončení rozhraní API.	Ano	Ne	Ne	Ne	Ne
<u>Posloupnost</u>	Posloupnost, ve které je tato uživatelská procedura volána relativně k jiným uživatelským procedurám.	Ano	Ne	Ne	Ne	Ne

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravo váno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
Sekce zabezpečení						
<u>DisableClientAMS</u>	Zakáže nebo povolí AMS pro připojení klienta ke správci front.	Ano	Ano	Ano	Ne	Ne
Sekce SSL						
<u>CDPCheckExtensions</u>	Určuje, zda se kanály SSL nebo TLS v tomto správci front pokusí zkontrolovat servery CDP, které jsou pojmenované v rozšířeních certifikátu bodu CrIDistributio n.	Ano	Ne	Ne	Ne	Ne
<u>CertificateLabel</u>	Jmenovka certifikátu pro definici kanálu.	Ano	Ne	Ne	Ne	Ne
<u>CertificateVal</u>	Určuje typ použitého ověření certifikátu.	Ano	Ne	Ne	Ne	Ne
<u>ClientRevocation-kontroly</u>	Určuje, jak je kontrola odvolání certifikátů konfigurován a, pokud volání connect klienta používá kanál SSL/ TLS.	Ano	Ne	Ne	Ne	Ne

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravo váno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
EncryptionPolicySuiteB	Určuje, zda kanál používá šifrování vyhovující standardu Suite-B a jaká úroveň síly se má použít.	Ano	Ne	Ne	Ne	Ne
Ověření OCSPAuthentication	Definuje chování produktu IBM MQ, je-li protokol OCSP povolen a kontrola odvolání OCSP není schopna určit stav odvolání certifikátu.	Ano	Ne	Ne	Ne	Ne
OCSPCheckExtensions	Řídí, zda produkt IBM MQ funguje na rozšíření certifikátu AuthorityInfo Access.	Ano	Ne	Ne	Ne	Ne
SSLCryptoHardware	Nastaví řetězec parametrů požadovaný ke konfiguraci kryptografického hardwaru PKCS #11 přítomným na systému.	Ano	Ne	Ne	Ne	Ne


Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nesprávně .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
SSLFipsRequired	Určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, je-li šifrování prováděno v produktu IBM MQ.	Ano	Ne	Ne	Ne	Ne
SSLHTTPProxyName	Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použit pro kontroly OCSP.	Ano	Ne	Ne	Ne	Ne
SSLKeyRepository	Umístění úložiště klíčů, které obsahuje digitální certifikát uživatele, v kmenového formátu.	Ano	Ne	Ne	Ne	Ne
PočetSSLKeyResetCount	Počet nezašifrovaných bajtů odeslaných a přijatých na kanál SSL nebo TLS, než je znovu vyjednán tajný klíč.	Ano	Ne	Ne	Ne	Ne
Sekce TCP						

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nesprávně .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
<u>ClntRcvBufferSize</u>	Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.	Ano	Ano	Ano	Ano	Ano
<u>ClntSndBufferSize</u>	Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.	Ano	Ano	Ano	Ano	Ano
<u>Časový limit připojení</u>	Počet sekund před pokusem o připojení k vypršení časového limitu socketu.	Ano	Ano	Ano	Ne	Ne
<u>IPAddressVersion</u>	Určuje protokol IP, který má být použit pro připojení kanálu.	Ano	Ne	Ne	Ano	Ano

Tabulka 9. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu mqclient.ini	Popis	C a nespravováno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
KeepAlive	Zapne nebo vypne funkci KeepAlive .	Ano	Ano	Ano	Ano	Ano
 Windows Library1	Pouze v systému Windows , název soketů DLL TCP/IP.	Ano	Ne	Ne	Ne	Ne

Pro klienta IBM MQ for HP Integrity NonStop Servermůžete použít sekce [TMF](#) a [TmfGateway](#) ke komunikaci s TMF/Gateway.

stanza CHANNELS konfiguračního souboru klienta

Použijte sekci CHANNELS k uvedení informací o kanálech klienta.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ MQI client viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Do stanzy CHANNELS mohou být zahrnuty následující atributy.

CCSID = číslo

Kódované číslo znakové sady, které má být použito.


Tento atribut lze číst z C, nespravovaných .NET, spravovaných .NETa spravovaných klientů XMS .NET .

Číslo CCSID je ekvivalentní parametru prostředí MQCCSID.

ChannelDefinitionDirectory = cesta

Cesta k adresáři se souborem obsahujícím tabulku definic kanálů klienta.

Tento atribut lze číst z C, nespravovaných .NET, spravovaných .NETa spravovaných klientů XMS .NET .

 U systémů Windows je standardní hodnotou adresář dat IBM MQ a adresář souborů protokolu, zpravidla C:\ProgramData\IBM\MQ.

  U systémů SYSTÉM UNIX a Linux je standardní hodnota /var/mqm.

Cesta k adresáři ChannelDefinitionje ekvivalentní s parametrem prostředí MQCHLLIB.

ChannelDefinitionFile = ***název_souboru*** | **AMQCLCHL.TAB**

Název souboru obsahujícího tabulku definic kanálů klienta.

Tento atribut lze číst z C, nespravovaných .NET, spravovaných .NETa spravovaných klientů XMS .NET .

Tabulka definic kanálů klienta je ekvivalentní parametru prostředí MQCHLTAB.

ReconDelay = (***prodleva*** [, ***rand***]) (***prodleva*** [, ***rand***]) ...

Atribut ReconDelay poskytuje administrativní volbu pro konfiguraci prodlevy opětného připojení pro klientské programy, které mohou automaticky znovu navázat spojení.

Tento atribut lze číst z C, nespravovaných .NET, IBM MQ classes for JMS, spravovaných .NETa spravovaných klientů XMS .NET .

Zde je příklad konfigurace:

ReconDelay=(1000,200)(2000,200)(4000,1000)

Příklad zobrazuje počáteční prodlevu o jednu sekundu s náhodným intervalem až 200 milisekund. Další prodleva je dvě sekundy plus náhodný interval až 200 milisekund. Všechna následující zpoždění jsou čtyři sekundy s náhodným intervalem až 1000 milisekund.

DefRecon = NO | YES | QMGR | DISABLED

Atribut DefRecon poskytuje administrativní volbu, která umožňuje klientským programům automaticky znovu navázat spojení nebo zakázat automatické opětovné připojení klientského programu, který byl napsán pro automatické nové připojení. Pokud program používá volbu, jako např. MQPMO_LOGICAL_ORDER, která není kompatibilní s opětovným připojením, můžete ji nastavit jako druhou.

Tento atribut lze číst z C, nespravovaných .NET, IBM MQ classes for JMS, spravovaných .NETa spravovaných klientů XMS .NET .

Třídy IBM MQ pro jazyk Java automatické opětovné připojování klientů nepodporují.

Interpretace voleb DefRecon závisí na tom, zda je hodnota MQCNO_RECONNECT_* nastavena také v klientském programu a jaká hodnota je nastavena.

Pokud se klientský program připojí k produktu MQCONNnebo nastaví volbu MQCNO_RECONNECT_AS_DEF pomocí příkazu MQCONNX, hodnota opětovného připojení nastavená hodnotou DefRecon se projeví. Není-li v programu nastavena žádná hodnota reconnect, nebo ve volbě DefRecon není program klienta automaticky znovu připojen.

NO

Pokud není přepsáno produktem MQCONNX, klient se automaticky nepřipojí automaticky.

YES

Pokud není přepsáno produktem MQCONNX, klient se znovu připojí automaticky.

QMGR

Pokud nebude přepsán produktem MQCONNX, klient se znovu připojí automaticky, ale pouze se stejným správcem front. Volba QMGR má stejný účinek jako MQCNO_RECONNECT_Q_MGR.

VYPNUTO

Opětovné připojení je zakázáno, i když je vyžádáno klientským programem pomocí volání modulu MQCONNX MQI.

Automatické opětovné připojení klienta závisí na dvou hodnotách:

- Volba opětovného připojení nastavená v aplikaci
- Hodnota **DefRecon** v souboru mqclient.ini

Tabulka 10. Automatické opětovné navázání spojení závisí na hodnotách nastavených v aplikaci a v souboru mqclient.ini .

Hodnota DefRecon v mqclient .ini	Volby opětovného připojení nastavené v aplikaci			
	MQCNO_RECONNE CT	MQCNO_RECONNECT_Q _MGR	MQCNO_RECONNECT_AS _DEF	MQCNO_RECONNECT_DIS ABLED
NO	YES	QMGR	NO	NO
YES	YES	QMGR	YES	NO
QMGR	YES	QMGR	QMGR	NO
VYPNUTO	NO	NO	NO	NO

MQReconnectTimeout

Časový limit v sekundách, který se má znovu připojit ke klientovi. Výchozí hodnota je 1800 sekund (30 minut).

Tento atribut může číst v jazyce C a nespravovaných klientů .NET a spravovaných klientů .NET .

Klienti produktu IBM MQ classes for JMS mohou určit časový limit pro opětovné připojení pomocí vlastnosti továrny připojení CLIENTRECONNECTTIMEOUT. Výchozí hodnota této vlastnosti je 1800 sekund (30 minut).

Klienti produktu IBM MQ classes for XMS .NET mohou určit časový limit opakovaného připojení s použitím následujících vlastností:

- Vlastnost továrny připojení CLIENTRECONTIMEOUT. Výchozí hodnota této vlastnosti je 1800 sekund (30 minut). Tato vlastnost je platná pouze pro spravovaný režim.
- Vlastnost XMSC.WMQ_CLIENT_RECONNECT_TIMEOUT. Výchozí hodnota této vlastnosti je 1800 sekund (30 minut). Tato vlastnost je platná pouze pro spravovaný režim.

ServerConnectionParms

Parametry ServerConnectionParms jsou ekvivalentní parametru prostředí MQSERVER a určují umístění serveru IBM MQ a komunikační metodu, která má být použita.

Tento atribut lze číst z C, nespravovaných .NET, spravovaných .NET a spravovaných klientů XMS .NET .

Atribut Parametry ServerConnectionParms definuje pouze jednoduchý kanál. Nelze ji použít k definování kanálu SSL nebo kanálu s uživatelskými procedurami kanálu. Je to řetězec formátu *ChannelName/TransportType/ConnectionName*, *ConnectionName* musí být plně kvalifikovaný název sítě. *ChannelName* nesmí obsahovat znak dopředného lomítka (/), protože tento znak se používá k oddělení názvu kanálu, typu transportu a názvu připojení.

Když se parametry ServerConnectionParms používají k definování kanálu klienta, použije se maximální délka zprávy 100 MB. Proto maximální velikost zprávy platná pro kanál je hodnota zadaná v kanálu SVRCONN na serveru.

Všimněte si, že lze vytvořit pouze jedno připojení kanálu klienta. Máte-li například dvě položky:

```
ServerConnectionParms=R1.SVRCONN/TCP/localhost(1963)
ServerConnectionParms=R2.SVRCONN/TCP/localhost(1863)
```

je použit pouze druhý z nich.

Jako seznam názvů pro uvedený typ transportu zadejte *ConnectionName* jako čárkami oddělený seznam názvů. Obecně je požadován pouze jeden název. Můžete zadat *více názvů hostitelů* , chcete-li konfigurovat více připojení se stejnými vlastnostmi. Připojení se zkoušejí v pořadí, ve kterém jsou uvedeny v seznamu připojení, dokud nebude spojení úspěšně ustanoveno. Není-li připojení úspěšné, klient se znovu spustí. Seznamy spojení jsou alternativou ke skupinám správců front pro konfiguraci připojení pro reconnectable clients.

Put1DefaultAlwaysSync = NE | ANO

Řídí chování volání funkce MQPUT1 s volbou MQPMO_RESPONSE_AS_Q_DEF.

Tento atribut lze číst o C, nespravovaných .NET, IBM MQ classes for Java a IBM MQ classes for JMS, spravovaných .NET a spravovaných klientech XMS .NET .

NO

Je-li parametr MQPUT1 nastaven na hodnotu MQPMO_SYNCPOINT, chová se jako MQPMO_ASYNC_RESPONSE. Podobně platí, že je-li parametr MQPUT1 nastaven s hodnotou MQPMO_NO_SYNCPOINT, chová se jako MQPMO_SYNC_RESPONSE. Toto je výchozí hodnota.

YES

Hodnota MQPUT1 se chová, jako by byla nastavena hodnota MQPMO_SYNC_RESPONSE , bez ohledu na to, zda je nastavena hodnota MQPMO_SYNCPOINT nebo MQPMO_NO_SYNCPOINT .

PasswordProtection = Kompatibilní | vždy | volitelné

V produktu IBM MQ 8.0 vám umožňuje nastavit chráněná hesla ve struktuře MQCSP raději než pomocí SSL nebo TLS.

Tento atribut lze číst o C, nespravovaných .NET, IBM MQ classes for Java a IBM MQ classes for JMS, spravovaných .NET a spravovaných klientech XMS .NET .

Ochrana heslem MQCSP je užitečná pro účely testování a vývoje, protože použití ochrany heslem MQCSP je jednodušší než nastavení šifrování SSL/TLS, ale ne jako zabezpečené. Další informace naleznete v tématu [Ochrana heslem MQCSP](#).

Související informace

[Připojení aplikací IBM MQ MQI ke správcům front](#)

stanza cesty ClientExitkonfiguračního souboru klienta

Pomocí oddílu Cesta ClientExit určete výchozí umístění kanálů kanálu na straně klienta.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ MQI client viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Následující atributy mohou být zahrnuty do stanzy ClientExitPath.

ExitsDefaultPath = řetězec

Určuje umístění 32bitového kanálu pro klienty.

Tento atribut lze číst z klientů C, nespravovaných .NET, spravovaných .NET, spravovaných klientů XMS .NET, IBM MQ classes for Java a IBM MQ classes for JMS . Klienti IBM MQ classes for Java a IBM MQ classes for JMS používají tento atribut k vyhledání 32bitových uživatelských procedur kanálu, které nejsou zapsány v produktu Java.

ExitsDefaultPath64 = řetězec

Určuje umístění 64bitových kanálů kanálů pro klienty.

Tento atribut lze číst z klientů C, nespravovaných .NET, spravovaných .NET, spravovaných klientů XMS .NET, IBM MQ classes for Java a IBM MQ classes for JMS . Klienti IBM MQ classes for Java a IBM MQ classes for JMS používají tento atribut k vyhledání 64bitových kanálů kanálů, které nejsou zapsány v produktu Java.

JavaExitsClassPath = řetězec

Hodnoty, které mají být přidány do cesty ke třídě při spuštění uživatelské procedury produktu Java . Tento parametr je ignorován ukončovacími programy v jiném jazyce.

Tento atribut lze číst klienty IBM MQ classes for Java a IBM MQ classes for JMS .

V konfiguračním souboru obslužného programu JMS je název cesty JavaExitsClassPath zadán standardním prefixem com.ibm.mq.cfg. a tento úplný název je také použit v systémové vlastnosti IBM WebSphere MQ 7.0 nebo novější. V parametru Verze 6.0 byl tento atribut zadán s použitím systémové vlastnosti com.ibm.mq.exitClasspath, která byla dokumentována v souboru README produktu Verze 6.0 . Použití objektu com.ibm.mq.exitClasspath bylo zamítnuto. Pokud jsou přítomny obě volby JavaExitsClassPath a exitClasspath , je JavaExitsClassPath poctěn. Je-li přítomen pouze použití exitClasspath , je stále dodržován v produktu IBM WebSphere MQ 7.0 nebo novějším.

stanza JMQUI konfiguračního souboru klienta

Sekce JMQUI slouží k určení konfiguračních parametrů pro rozhraní JMQUI (Message Queuing Interface) produktu Java využívaných produkty IBM MQ classes for Java a IBM MQ classes for JMS.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ MQI client viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Následující atribut může být zahrnut do stanzy JMQUI:

useMQCSPauthentication = NO | YES

Řídí, zda aplikace IBM MQ classes for Java a IBM MQ classes for JMS mají při ověřování u správce front používat režim kompatibility nebo režim ověřování MQCSP.

Tento atribut lze číst klienty IBM MQ classes for Java a IBM MQ classes for JMS .

Tento atribut může mít následující hodnoty:

NO

Při ověřování u správce front použijte režim kompatibility. Toto je výchozí hodnota.

YES

Při ověřování u správce front použít režim ověřování MQCSP.

Další informace o režimu kompatibility a režimu ověření MQCSP naleznete v tématu [Ověření připojení pomocí klienta Java](#).

Windows Stanzy LU62, NETBIOS a SPX v konfiguračním souboru klienta

Pouze v systémech Windows použijte tyto sekce k určení konfiguračních parametrů pro zadané síťové protokoly.

stanza LU62

Sekce LU62 se používá k určení konfiguračních parametrů protokolu SNA LU 6.2 . Do této stanzy mohou být zahrnuty následující atributy:

Library1 = DLLName | WCPI32

Název knihovny APPC DLL.

Library2 = DLLName | WCPI32

Stejně jako Library1, používá se, pokud je kód uložen ve dvou samostatných knihovnách.

TPName

Název transakčního programu, který má být spuštěn na vzdáleném serveru.

Sekce NETBIOS

Použijte sekci NETBIOS k uvedení konfiguračních parametrů protokolu NetBIOS . Do této stanzy mohou být zahrnuty následující atributy:

AdapterNum = číslo | 0

Číslo adaptéru sítě LAN.

Library1 = DLLName | NETAPI32

Název knihovny DLL NetBIOS .

LocalName = název

Název, pod kterým je tento počítač znám v síti LAN.

Jedná se o ekvivalent parametru prostředí MQNAME.

NumCmds = číslo | 1

Počet příkazů k přidělení.

NumSess = číslo | 1

Počet relací k přidělení.

Sekce SPX

Použijte sekci SPX k určení konfiguračních parametrů protokolu SPX. Do této stanzy mohou být zahrnuty následující atributy:

BoardNum = číslo | 0

Číslo adaptéru LAN.

KeepAlive = YES | NO

Vypněte funkci KeepAlive zapnutou nebo vypnutou.

KeepAlive = YES způsobí, že SPX bude pravidelně kontrolovat, zda je druhý konec připojení stále dostupný. Není-li tomu tak, kanál je uzavřen.

Library1 = *DLLName* | WSOCK32.DLL

Název knihovny SPX DLL.

Library2 = *DLLName* | WSOCK32.DLL

Totéž jako Library1, používá se, pokud je kód uložen ve dvou samostatných knihovnách.

Socket = číslo | 5E86

Číslo soketu SPX v hexadecimální notaci.

stanza **MessageBuffer** konfiguračního souboru klienta

Použijte sekci MessageBuffer k uvedení informací o vyrovnávacích pamětech zpráv.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ MQI client viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Do sekce MessageBuffer mohou být zahrnuty následující atributy:

MaximumSize = celé_číslo | 1

Velikost vyrovnávací paměti dopředného čtení v kilobajtech, v rozsahu 1-999 999.

Tento atribut lze číst příkazem C, nespravovanými klienty .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaným produktem .NETa spravovanými klienty XMS .NET .

Existují následující speciální hodnoty:

-1

Klient určí příslušnou hodnotu.

0

Čtení napřed je zakázáno pro klienta.

PurgeTime = celé_číslo | 600

Interval, v sekundách, po jehož uplynutí jsou vyprázdněny zprávy ponechané ve vyrovnávací paměti dopředného čtení.

Tento atribut lze číst příkazem C, nespravovanými klienty .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaným produktem .NETa spravovanými klienty XMS .NET .

Pokud aplikace klienta vybírá zprávy založené na hodnotě MsgId nebo CorrelId, je možné, že vyrovnávací paměť dopředného čtení může obsahovat zprávy odeslané klientovi s dříve požadovanou hodnotou MsgId nebo CorrelId. Tyto zprávy by pak uvízly v vyrovnávací paměti dopředného čtení, dokud nebude příkaz MQGET zadán s příslušnou hodnotou MsgId nebo CorrelId. Zprávy z vyrovnávací paměti dopředného čtení můžete vyprázdnit nastavením parametru PurgeTime. Všechny zprávy, které zůstaly ve vyrovnávací paměti čtení napřed déle, než je interval mazání, jsou automaticky vyprázdněny. Tyto zprávy již byly odebrány z fronty na správci front, takže pokud nejsou procházeny, jsou ztraceny.

Platný rozsah je v rozsahu 1-999 999 sekund, nebo speciální hodnota 0, což znamená, že nedochází k žádnému vyprázdnění.

UpdatePercentage = celé_číslo | -1

Hodnota aktualizace v procentech, v rozsahu 1-100, která se používá při výpočtu prahové hodnoty k určení toho, kdy klientská aplikace vytváří nový požadavek na server. Speciální hodnota -1 označuje, že klient určí příslušnou hodnotu.

Tento atribut lze číst příkazem C, nespravovanými klienty .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaným produktem .NETa spravovanými klienty XMS .NET .

Klient pravidelně odesílá požadavek na server a uvádí, kolik dat spotřebovala klientská aplikace. Požadavek se odešle, když počet bajtů, *n*, načtený klientem prostřednictvím volání MQGET překročí prahovou hodnotu *T*. *n* se vynuluje pokaždé, když se odešle nový požadavek na server.

Prahová hodnota T se vypočítá takto:

$$T = \text{Upper} - \text{Lower}$$

Horní hodnota je stejná jako velikost vyrovnávací paměti dopředného čtení určená atributem `MaximumSize`, v kilobajtech. Jeho výchozí hodnota je 100 Kb.

Dolní je menší než horní, a je určen atributem `UpdatePercentage`. Tento atribut je číslo v rozsahu 1-100 a má výchozí hodnotu 20. Nižší hodnota se vypočítá takto:

$$\text{Lower} = \text{Upper} \times \text{UpdatePercentage} / 100$$

Příklad 1:

Atributy `MaximumSize` a `UpdatePercentage` mají výchozí nastavení hodnot 100 Kb a 20 kB.

Klient volá příkaz `MQGET` k načtení zprávy a provádí to opakovaně. To pokračuje, dokud příkaz `MQGET` nespotřebuje n bajtů.

Použití výpočtu

$$T = \text{Upper} - \text{Lower}$$

T je $(100-20) = 80$ kB.

Když tedy volání `MQGET` odebrala 80 kb z fronty, klient automaticky vytvoří nový požadavek.

Příklad 2:

Atribut `MaximumSize` má výchozí hodnotu 100 Kb a hodnota 40 je vybrána pro hodnotu `UpdatePercentage`.

Klient volá příkaz `MQGET` k načtení zprávy a provádí to opakovaně. To pokračuje, dokud příkaz `MQGET` nespotřebuje n bajtů.

Použití výpočtu

$$T = \text{Upper} - \text{Lower}$$

T je $(100-40) = 60$ kB

Když tedy volání `MQGET` odebrala 60 kB z fronty, klient automaticky vytvoří nový požadavek. To je dříve než v případě, kde byly použity výchozí hodnoty.

Proto výběr větší prahové hodnoty T má tendenci snížit četnost, při které jsou požadavky odesílány z klienta na server. Naopak, výběr menší prahové hodnoty T má tendenci zvýšit četnost požadavků, které jsou odesílány z klienta na server.

Výběr velké prahové hodnoty T však může znamenat, že zvýšení výkonu čtení napřed je sníženo, protože se může zvýšit pravděpodobnost, že se vyrovnávací paměť dopředného čtení stane prázdnou. Když se to stane, může dojít k pozastavení volání `MQGET` a čeká na data, která dorazí ze serveru.

stanza PreConnect konfiguračního souboru klienta

Použijte sekci `PreConnect` ke konfiguraci uživatelské procedury `PreConnect` v souboru `mqclient.ini`.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ `MQI client` viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Do sekce `PreConnect` mohou být zahrnuty následující atributy:

Data = < URL >

Adresa URL úložiště, kde jsou uloženy definice připojení.

Tento atribut může číst v jazyce C a nespravovaných klientů `.NET`.

Například při použití serveru LDAP:

```
Data = ldap://myLDAPServer.com:389/cn=wmq,ou=ibm,ou=com
```

Function = <myFunc>

Název funkčního vstupního bodu do knihovny, která obsahuje výstupní kód PreConnect .

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Definice funkce dodržuje prototyp uživatelské procedury PreConnect [MQ_PRECONNECT_EXIT](#).

Maximální délka tohoto pole je MQ_EXIT_NAME_LENGTH.

Module = <amqldapi>

Název modulu obsahujícího kód ukončení rozhraní API.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Pokud toto pole obsahuje úplnou cestu k modulu, použije se tak, jak je.

Sequence = <pořadové_číslo>

Posloupnost, ve které je tato uživatelská procedura volána relativně k jiným uživatelským procedurám. Uživatelská procedura s nízkým pořadovým číslem se volá před ukončením s vyšším pořadovým číslem. Není třeba, aby sekvenční číslování vstupů bylo spojováno; posloupnost 1, 2, 3 má stejný výsledek jako posloupnost 7, 42, 1096. Tento atribut je nepodepsaná číselná hodnota.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

V souboru mqclient.ini může být definováno více oddílů PreConnect . Pořadí zpracování každé procedury je určeno atributem Posloupnost stanzy.

Související informace

[Odkazování na definice připojení pomocí předání před připojením z úložiště](#)

Sekce zabezpečení konfiguračního souboru klienta

Použijte sekci Zabezpečení, abyste zablokovali nebo povolili AMS pro připojení klienta ke správci front.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ MQI client viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Následující atribut může být zahrnut ve stanze zabezpečení:

DisableClientAMS = NO|YES

Atribut DisableClientAMS vám umožňuje zakázat IBM MQ Advanced Message Security (AMS), pokud používáte klienta Verze 7.5 nebo novější pro připojení ke správci front ze starší verze produktu a je hlášena chyba 2085 (MQRC_UNKNOWN_OBJECT_NAME) .

V produktu Verze 7.5 je produkt IBM MQ Advanced Message Security (AMS) automaticky aktivován v klientovi IBM MQ a při výchozím nastavení se klient pokusí zkontrolovat zásady zabezpečení pro objekty ve správci front. Nicméně servery ve starších verzích produktu, například Verze 7.1, nemají povoleny AMS a způsobí chybu 2085 (MQRC_UNKNOWN_OBJECT_NAME) chyby.

Následující příklady ukazují, jak použít atribut DisableClientAMS :

- Chcete-li zakázat AMS:

```
Security:  
DisableClientAMS=Yes
```

- Chcete-li povolit AMS:

```
Security:  
DisableClientAMS=No
```

Tento atribut může číst klienti C, IBM MQ classes for Java a IBM MQ classes for JMS .

Související informace

[Zakázání rozšířeného zabezpečení zpráv na straně klienta](#)

stanza SSL konfiguračního souboru klienta

Použijte sekci SSL k uvedení informací o použití SSL nebo TLS.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ MQI client viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Následující atributy mohou být obsaženy ve stanze SSL:

CDPCheckExtensions= YES | NO

CDPCheckExtensions uvádí, zda se kanály SSL nebo TLS v tomto správci front pokouší zkontrolovat servery CDP, které jsou pojmenované v rozšířených certifikátu bodu CrlDistributionPoint.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Tento atribut může mít následující hodnoty:

- AN0: Kanály SSL nebo TLS se snaží zkontrolovat servery CDP za účelem určení, zda je digitální certifikát odvolán.
- N0: Kanály SSL nebo TLS se nesnažte kontrolovat servery CDP. Tato hodnota je výchozí.

CertificateLabel = řetězec

Jmenovka certifikátu pro definici kanálu.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Další informace najdete v tématu [Označení certifikátu \(CERTLABL\)](#).

CertificateValPolicy = řetězec

Určuje typ použitého ověření certifikátu.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Tento atribut může mít následující hodnoty:

ANY

Použijte jakoukoli zásadu ověření platnosti certifikátu podporovanou základní zabezpečenou knihovnou socketů. Toto nastavení je výchozí nastavení.

RFC5280

Používejte pouze ověření certifikátu, které je v souladu s normou RFC 5280.

ClientRevocationChecks = REQUIRED | OPTIONAL | DISABLED


Určuje, jak je kontrola odvolání certifikátů konfigurována, pokud volání connect klienta používá kanál SSL/TLS. Viz též [OCSPAuthentication](#).

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Tento atribut může mít následující hodnoty:

POŽADOVÁNO (výchozí)

Pokusí se o načtení konfigurace odvolání certifikátu z tabulky CCDT a provedení kontroly odvolání, jak je nakonfigurováno. Pokud nelze soubor tabulky CCDT otevřít nebo není možné ověřit certifikát (protože není k dispozici protokol OCSP nebo CRL, například), volání MQCONN selže. Pokud tabulka CCDT neobsahuje žádnou konfiguraci odvolání, neprovádí se žádná kontrola odvolání, ale to nezpůsobí selhání kanálu.

 V systému Windows můžete také použít Active Directory pro kontrolu odvolání CRL. Pro kontrolu odvolání OCSP nelze použít volbu Active Directory .

Volitelný

Co se týče REQUIRED, ale pokud není možné načíst konfiguraci odvolání certifikátu, kanál se nenezdáří.

VYPNUTO

Při načítání konfigurace odvolání certifikátu z tabulky CCDT nebyl proveden žádný pokus o načtení konfigurace odvolání certifikátu a nebyla provedena kontrola odvolání certifikátů.

Poznámka: Pokud používáte volání MQCONNX namísto volání MQCONN, můžete se rozhodnout pro zadání záznamů ověřovacích informací (MQAIR) prostřednictvím struktury MQSCO. Výchozí chování s MQCONNX se proto nenezdaří, pokud soubor CCDT nelze otevřít, ale předpokládá se, že dodáte aplikaci MQAIR (i když se rozhodnete, že ji nechcete provést).

EncryptionPolicySuiteB = řetězec

Určuje, zda kanál používá šifrování vyhovující standardu Suite-B a jaká úroveň síly se má použít.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Tento atribut může mít následující hodnoty:

ŽÁDNÉ

Šifrování vyhovující standardu Suite-B se nepoužívá. Toto nastavení je výchozí nastavení.

128_BIT,192_BIT

Nastavuje sílu zabezpečení na úroveň 128-bit a 192 bitů.

128_BIT

Nastavuje sílu zabezpečení na 128bitovou úroveň.

192_BIT

Nastaví odolnost zabezpečení na 192bitovou úroveň.

OCSPAuthentication = OPTIONAL | REQUIRED | WARN

Definuje chování produktu IBM MQ , je-li protokol OCSP povolen a kontrola odvolání OCSP není schopna určit stav odvolání certifikátu. Viz též [ClientRevocationChecks](#).

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Tento atribut může mít následující hodnoty:

Volitelný

Je přijat libovolný certifikát se stavem odvolání, který nelze určit pomocí kontroly OCSP, a nebude generována žádná varování ani chybová zpráva. Připojení SSL nebo TLS bude pokračovat, jako by nebyla provedena kontrola odvolání.

POVINNÉ

Kontrola OCSP musí vést k definitivnímu výsledku odvolání pro každý certifikát SSL nebo TLS, který je kontrolován. Jakýkoliv certifikát SSL nebo TLS se stavem odvolání, který nelze ověřit, je odmítnut s chybovou zprávou. Jsou-li povoleny zprávy událostí SSL správce front, vygeneruje se zpráva MQRC_CHANNEL_SSL_ERROR s generovanou hodnotou ReasonQualifier MQRQ_SSL_HANDSHAKE_ERROR. Připojení je zavřeno.

Tato hodnota je výchozí hodnotou.

WARN

Pokud není kontrola odvolání OCSP schopna určit stav odvolání certifikátů SSL nebo TLS, je v protokolech chyb správce front hlášeno varování. Jsou-li povoleny zprávy událostí SSL správce front, vygeneruje se zpráva MQRC_CHANNEL_SSL_WARNING s hodnotou ReasonQualifier objektu MQRQ_SSL_UNKNOWN_REVOCATION. Připojení může pokračovat.

OCSPCheckExtensions = YES | NO

Řídí, zda produkt IBM MQ funguje na rozšíření certifikátu AuthorityInfoAccess.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Je-li hodnota nastavena na NO, produkt IBM MQ ignoruje rozšíření certifikátu AuthorityInfoAccess a nepokusí se o kontrolu zabezpečení OCSP. Výchozí hodnota je YES.

SSLCryptoHardware = řetězec

Nastaví řetězec parametrů požadovaný ke konfiguraci kryptografického hardwaru PKCS #11 přítomným na systému.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Určete řetězec v následujícím formátu: GSK_PKCS11 = *cesta k ovladači a název souboru ; popisek tokenu ; heslo tokenu ; nastavení symetrických šifer ;*

Například: GSK_PKCS11=/usr/lib/pkcs11/
PKCS11_API.so;tokenlabel;passwd;SYMMETRIC_CIPHER_ON

Cesta k ovladači je absolutní cesta ke sdílené knihovně poskytující podporu pro kartu PKCS #11 . Název souboru ovladače je název sdílené knihovny. Příklad hodnoty požadované pro cestu k ovladači PKCS #11 a název souboru je /usr/lib/pkcs11/PKCS11_API . so. Chcete-li přistupovat k symetrickým operacím šifer prostřednictvím sady GSKit, zadejte parametr nastavení symetrického šifry. Tento parametr může mít jednu z následujících hodnot:

SYMMETRIC_CIPHER_VYPNUTO

Nepřístupovat k symetrickým operacím šifry. Toto nastavení je výchozí nastavení.

SYMMETRIC_CIPHER_ON

Přístup k symetrickým šifrováním.

Maximální délka řetězce je 256 znaků. Výchozí hodnota je prázdná. Uvedete-li řetězec, který není ve správném formátu, vygeneruje se chyba.

SSLFipsRequired = YES | NO

Určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, je-li šifrování prováděno v produktu IBM MQ.

Tento atribut lze číst v jazyce C a nespravovaných klientů .NET .

Je-li konfigurován kryptografický hardware, použité šifrovací moduly jsou moduly, které poskytují hardwarový produkt. To může být, nebo nemusí, být FIPS certifikováno na konkrétní úroveň, v závislosti na použití hardwarového produktu.

SSLHTTPProxyName = řetězec

Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použít pro kontroly OCSP. Za touto adresou může následovat volitelné číslo portu uzavřené v závorkách. Pokud číslo portu neurčíte, zvolí se výchozí port HTTP, který má číslo 80.

Tento atribut lze číst v jazyce C a nespravovaných klientů .NET .

Na platformách HP-UX PA-RISC a Sun Solaris SPARC a pro 32bitové klienty na systému AIX může být síťová adresa pouze adresou IPv4 ; na jiných platformách může být adresa IPv4 nebo IPv6 .

Tento atribut může být nezbytný, pokud například ochranná bariéra brání přístupu k adrese URL odpovídajícího modulu OCSP.

SSLKeyRepository = název_cesty

Umístění úložiště klíčů, které obsahuje digitální certifikát uživatele, v kmenového formátu. To znamená, že obsahuje úplnou cestu a název souboru bez přípony.

Tento atribut lze číst v jazyce C a nespravovaných klientů .NET .

SSLKeyResetCount = celé_číslo | 0

Počet nezašifrovaných bajtů odeslaných a přijatých na kanál SSL nebo TLS, než je znovu vyjednáno tajný klíč.

Tento atribut lze číst v jazyce C a nespravovaných klientů .NET .

Hodnota musí být v rozsahu 0 až 999999999.

Předvolená hodnota je 0, což znamená, že tajné klíče nejsou nikdy znovu vyjednávány.

Určíte-li hodnotu 1-32768, budou kanály zabezpečení SSL nebo TLS používat počet obnovení tajných klíčů 32768 (32Kb). Tím se vyhnete přílišnému resetování klíčů, které by se mohlo vyskytnout u hodnot malých tajných klíčů.

Sekce TCP konfiguračního souboru klienta

stanzu TCP použijte k uvedení konfiguračních parametrů síťového protokolu TCP.

Poznámka: Popis každého atributu této stanzy označuje, kteří klienti IBM MQ mohou číst tento atribut. Informace k souhrnné tabulce pro všechny stanzy konfiguračního souboru IBM MQ MQI client viz [Které atributy IBM MQ lze číst jednotlivými klienty](#).

Následující atributy mohou být zahrnuty do stanzy TCP:

ClntRcvBuffSize = číslo | 0

Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.

Tento atribut lze číst příkazem C, nespravovanými klienty .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaným produktem .NETa spravovanými klienty XMS .NET .

Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, a to na rozdíl od velikosti vyrovnávací paměti, které jsou opraveny produktem IBM MQ. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

ClntSndBuffSize = číslo | 0

Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.

Tento atribut lze číst příkazem C, nespravovanými klienty .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaným produktem .NETa spravovanými klienty XMS .NET .

Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, a to na rozdíl od velikosti vyrovnávací paměti, které jsou opraveny produktem IBM MQ. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

Connect_Timeout = číslo

Počet sekund před pokusem o připojení k vypršení časového limitu soketu. Výchozí hodnota nula určuje, že časový limit připojení neexistuje.

Tento atribut může číst klienti C, nespravovaný .NET, IBM MQ classes for Javaa IBM MQ classes for JMS .

Proces kanálu produktu IBM MQ se připojuje přes neblokující sokety. Pokud tedy druhý konec zásuvky není připraven, funkce connect () se vrátí okamžitě s hodnotou *EINPROGRESS* nebo *EWOULDBLOCK* . Po této operaci bude pokus o připojení znovu proveden až do celkového počtu 20 takových pokusů, je-li hlášena chyba komunikace.

Je-li parametr Connection_Timeout nastaven na jinou hodnotu než nula, produkt IBM MQ čeká na určené časové období prostřednictvím volání select (), aby se mohl soket připravit. Tím se zvyšuje šance na úspěch následného volání connect (). Tato volba může být užitečná v situacích, kdy by připojení vyžadovalo určité čekací období kvůli vysokému zatížení na síti.

Mezi parametry Connect_Timeout, ClntSndBuffSizea ClntRcvBuffSize neexistuje žádný vztah.

IPAddressVersion = MQIPADDR_IPV4 | MQIPADDR_IPV6

Určuje protokol IP, který má být použit pro připojení kanálu.

Tento atribut lze číst z C, nespravovaných .NET, spravovaných .NETa spravovaných klientů XMS .NET .

Má možné řetězce hodnot MQIPADDR_IPV4 nebo MQIPADDR_IPV6. Tyto hodnoty mají stejný význam jako IPV4 a IPV6 v **ALTER QMGR IPADDRV**.

KeepAlive = YES | NO

Vypněte funkci KeepAlive zapnutou nebo vypnutou. KeepAlive=ANO způsobí, že TCP/IP pravidelně kontroluje, zda je druhý konec připojení stále dostupný. Není-li tomu tak, kanál je uzavřen.

Tento atribut lze číst příkazem C, nespravovanými klienty .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaným produktem .NETa spravovanými klienty XMS .NET .

Windows **Library1 = DLLName | WSOCK32**

(pouze Windows) Název knihovny DLL soketů TCP/IP.

Tento atribut může číst v jazyce C a nespravovaných klientů .NET .

Sekce TMF a TmfGateway

Použijte sekce TMF a TMF/Gateway k uvedení požadovaných konfiguračních parametrů pro klienta IBM MQ pro produkt HP Integrity NonStop Server pro komunikaci s TMF/Gateway.

Chcete-li použít nástroj HP NonStop Transaction Management Facility (TMF), musíte definovat sekci TMF a jednu stanzu TmfGateway pro každého správce front, se kterým komunikujete. Všechny hodnoty jsou odvozeny z vaší konfigurace.

Produkt IBM MQ poskytuje TMF/Gateway, která je spuštěna v prostředí Pathway.

Sekce TMF

PathMon = *název*

Název vámi definovaného procesu Pathmon, který definuje třídy serveru pro TMF/Gateway.

stanza TmfGateway

Do této stanzy mohou být zahrnuty následující atributy:

QManager = *název*

Název správce front.

Server = *název*

Název třídy serveru pro TMF/Gateway nakonfigurovanou pro daného správce front.

Příklad

Zde je příklad objektu stanza TMF, který je definován se dvěma stanzami TmfGateway pro dva různé správce front na různých serverech:

```
TMF :  
PathMon=$PSD1P  
  
TmfGateway:  
QManager=MQ5B  
Server=MQ-MQ5B  
  
TmfGateway:  
QManager=MQ5C  
Server=MQ-MQ5C
```

Související pojmy

[“Přehled procesu brány” na stránce 516](#)

Produkt HP NonStop Transaction Management Facility (TMF) poskytuje služby, které umožňují procesu brány zaregistrovat se jako správce prostředků. Proces IBM WebSphere MQ for HP Integrity NonStop Server poskytovaný TMF/Gateway běží pod cestou Pathway.

[“Konfigurace inicializačního souboru klienta” na stránce 518](#)

Pokud používáte nástroj HP NonStop Transaction Management Facility (TMF), musíte mít inicializační soubor klienta IBM MQ , abyste umožnili klientovi IBM MQ pro přístup HP Integrity NonStop Server k bráně TMF Gateway.

Použití proměnných prostředí IBM MQ

Tento oddíl popisuje proměnné prostředí, které lze použít s aplikacemi produktu IBM MQ MQI client .


Proměnné prostředí můžete použít těmito způsoby:

- Nastavením proměnných ve vašem profilu systému provedete trvalou změnu.

- Vydejte příkaz z příkazového řádku, chcete-li provést změnu pouze pro tuto relaci
- Chcete-li dát jedné nebo více proměnným konkrétní hodnotu závislou na spuštěné aplikaci, přidejte příkazy do skriptového souboru příkazu použitého aplikací

IBM MQ používá výchozí hodnoty pro ty proměnné, které jste nenastavili.

Příkazy jsou k dispozici na všech platformách IBM MQ MQI client , pokud není uvedeno jinak.

Poznámka:  Produkt IBM MQ for z/OS nepodporuje žádné proměnné prostředí IBM MQ . Používáte-li tuto platformu jako server, viz [Tabulka definic kanálů klienta](#) , kde naleznete informace o tom, jak je tabulka definic kanálů klienta generována na z/OS. Na platformě klienta můžete stále používat proměnné prostředí IBM MQ .

Pro každou proměnnou prostředí použijte příkaz příslušný pro vaši platformu k zobrazení aktuálního nastavení nebo k resetování hodnoty proměnné.

V systému Windows použijte následující příkazy:

- Chcete-li odebrat hodnotu proměnné prostředí, použijte příkaz SET MQSERVER=
- Chcete-li zobrazit aktuální nastavení proměnné prostředí, použijte příkaz SET MQSERVER
- Chcete-li zobrazit všechny proměnné prostředí pro relaci, použijte příkaz set

V systémech SYSTÉM UNIX a Linux použijte následující příkazy:

- Chcete-li odebrat hodnotu proměnné prostředí, použijte příkaz unset MQSERVER
- Chcete-li zobrazit aktuální nastavení proměnné prostředí, použijte příkaz echo \$MQSERVER
- Chcete-li zobrazit všechny proměnné prostředí pro relaci, použijte příkaz set

Informace o jednotlivých proměnných naleznete v následujících dílčích tématech:

Související pojmy

“Konfigurace klienta pomocí konfiguračního souboru” na stránce 47

Nakonfigurujte své klienty pomocí atributů v textovém souboru. Tyto atributy mohou být přepsány proměnnými prostředí nebo jinými způsoby specifickými pro platformu.

Související informace

[Proměnné prostředí](#)

MQCCSID

Hodnota MQCCSID určuje číslo kódované znakové sady, které má být použito, a přepíše hodnotu CCSID, se kterou byl server konfigurován.

Další informace najdete v tématu [Výběr identifikátoru kódové sady znaků klienta nebo serveru \(CCSID\)](#) .

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Pro Windows:

```
SET MQCCSID=number
```

- Pro systémy SYSTÉM UNIX a Linux :

```
export MQCCSID=number
```

-  Pro IBM i:

```
ADDENVVAR ENVVAR(MQCCSID) VALUE(number)
```


MQCERTLABL.

Soubor MQCERTLABL určuje popis certifikátu pro definici kanálu.

Další informace najdete v tématu [Označení certifikátu \(CERTLABL\)](#).

MQCERTVPOL

Modul MQCERTVPOL určuje použitou zásadu ověření certifikátu.

Další informace o zásadách ověření platnosti certifikátů v produktu IBM MQ najdete v tématu [Zásady ověření certifikátu v produktu IBM MQ](#).

Tato proměnná prostředí potlačí nastavení *CertificateValPolicy* ve stanze SSL na souboru ini klienta. Proměnná může být nastavena na jednu ze dvou hodnot:

ANY

Použijte jakoukoli zásadu ověření platnosti certifikátu podporovanou základní zabezpečenou knihovnou socketů.

RFC5280

Používejte pouze ověření certifikátu, které je v souladu s normou RFC 5280.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Pro Windows:

```
SET MQCERTVPOL= value
```

- Pro systémy SYSTÉM UNIX a Linux :

```
export MQCERTVPOL= value
```





-  Pro IBM i:

```
ADDENVVAR ENVVAR(MQCERTVPOL) VALUE(value)
```





MQCHLLIB

MQCHLLIB uvádí cestu k adresáři se souborem obsahujícím tabulku definic kanálů klienta (CCDT). Soubor je vytvořen na serveru, ale lze jej zkopírovat na pracovní stanici IBM MQ MQI client .

Není-li parametr MQCHLLIB nastaven, je cesta pro klienta standardně nastavena na:

-  Pro Windows: `MQ_INSTALLATION_PATH`
-   Pro systémy SYSTÉM UNIX a Linux : `/var/mqm/`
-  Pro IBM i: `/QIBM/UserData/mqm/`

Pro příkazy `crtmqm` a `strmqm` je cesta standardně nastavena na jednu ze dvou sad cest. Je-li nastavena hodnota `datapath` , výchozí cesta je nastavena na jednu z první sady. Není-li parametr `datapath` nastaven, výchozí cesta je nastavena na jednu z druhé sady.

-  Pro Windows: `datapath\@ipcc`
-   Pro systémy SYSTÉM UNIX a Linux : `datapath/@ipcc`
-  Pro IBM i: `datapath/&ipcc`

Nebo:

-  Pro Windows: `MQ_INSTALLATION_PATH\data\qmgrs\qmgrname\@ipcc`

- **Linux** **UNIX** Pro systémy SYSTÉM UNIX a Linux : /prefix/qmgrs/qmgrname/@ipcc
- **IBM i** ProIBM i:/prefix/qmgrs/qmgrname/&ipcc

kde:

- `MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .
- Je-li tento parametr zadán, hodnota `datapath` je hodnota DataPath definovaná ve stanze správce front.
- `prefix` je hodnota Předpona definovaná ve stanze správce front. Předpona je obvykle /var/mqm na platformách SYSTÉM UNIX a Linux **IBM i** a /QIBM/UserData/mqm/ na IBM i.
- `qmgrname` je hodnota atributu Directory definovaná ve stanze správce front. Hodnota může být odlišná od názvu skutečného správce front. Hodnota mohla být změněna tak, aby nahradila speciální znaky.
- Oddíl správce front je definován v souboru `mq5.ini` na **IBM i** IBM, UNIXa Linux, a v registru v systému Windows

Notes:

1. **z/OS** Používáte-li jako svůj server IBM MQ for z/OS , musí být soubor uložen na pracovní stanici klienta IBM MQ .
2. Je-li nastavena hodnota, MQCHLLIB potlačí cestu použitou k umístění tabulky CCDT.
3. Proměnné prostředí, jako např. MQCHLLIB, mohou být omezeny na proces nebo úlohu nebo celosystémově specifické, v závislosti na platformě.
4. Nastavíte-li na serveru celý systém MQCHLLIB na úrovni systému, nastaví stejnou cestu k souboru CCDT pro všechny správce front na serveru. Pokud nenastavíte proměnnou prostředí MQCHLLIB , cesta se pro jednotlivé správce front liší. Správci front čtou hodnoty MQCHLLIB, pokud jsou nastaveny, buď na příkazu **crtmqm** , nebo na příkaz **strmqm** .
5. Pokud na jednom serveru vytvoříte více správců front, je tento rozdíl důležitý z následujících důvodů. Nastavíte-li systém MQCHLLIB v celém systému, bude každý správce front aktualizovat stejný soubor CCDT. Soubor obsahuje definice připojení klienta ze všech správců front na serveru. Pokud existuje stejná definice na více správcích front, SYSTEM . DEF . CLNTCONN například, obsahuje nejnovější definici. Při vytvoření správce front je v tabulce CCDT aktualizován produkt MQCHLLIB , pokud je nastaven na hodnotu SYSTEM . DEF . CLNTCONN . Aktualizace přepíše SYSTEM . DEF . CLNTCONN vytvořený jiným správcem front. Pokud jste upravili dřívější definici, vaše úpravy budou ztraceny. Z tohoto důvodu musíte zvážit nalezení alternativ k nastavení MQCHLLIB jako proměnné prostředí celého systému na serveru.
6. Volba MQSC a PCF NOREPLACE v definici připojení klienta nekontroluje obsah souboru CCDT. Je nahrazena definice kanálu připojení klienta se stejným názvem, který byl dříve vytvořen, ale nikoli tímto správcem front, bez ohledu na volbu NOREPLACE . Pokud definice byla dříve vytvořena stejným správcem front, definice se nenahradí.
7. Příkaz **rcrmqobj** -t clchltab odstraní a znovu vytvoří soubor CCDT. Soubor bude znovu vytvořen pouze s definicemi připojení klienta vytvořenými ve správci front, proti kterému je příkaz spuštěn.
8. Ostatní příkazy, které aktualizují CCDT, upravují pouze kanály připojení klienta se stejným názvem kanálu. Ostatní kanály připojení klienta v souboru se nezmění.
9. Cesta pro MQCHLLIB nevyžaduje uvozovky.

Příklady

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- **Windows** ProWindows:

```
SET MQCHLLIB=pathname
```

Příklad:

```
SET MQCHLLIB=C:\wmqtest
```

- **Linux** **UNIX** Pro systémy SYSTÉM UNIX a Linux :

```
export MQCHLLIB=pathname
```

- **IBM i** ProIBM i:

```
ADDENVVAR ENVVAR(MQCHLLIB) VALUE(pathname)
```

KARTA MQCHLTAB

Hodnota MQCHLTAB určuje název souboru, který obsahuje tabulku definic kanálů klienta (ccdt). Výchozí název souboru je AMQCLCHL.TAB.

Další informace o tom, kde je tabulka definic kanálů klienta umístěna na serveru, viz [“Tabulka definic kanálů klienta”](#) na stránce 37.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- zapWindows:

```
SET MQCHLTAB=filename
```

- V systémech SYSTÉM UNIX a Linux:

```
export MQCHLTAB=filename
```

- **IBM i** zapIBM i:

```
ADDENVVAR ENVVAR(MQCHLTAB) VALUE(filename)
```

Příklad:

```
SET MQCHLTAB=ccdf1.tab
```

Stejným způsobem jako pro klienta určuje proměnná prostředí MQCHLTAB na serveru název tabulky definic kanálů klienta.

MQIPADDRV

MQIPADDRV určuje, který protokol IP má být použit pro připojení kanálu. Má možné řetězcové hodnoty "MQIPADDR_IPv4" nebo "MQIPADDR_IPv6". Tyto hodnoty mají stejný význam jako IPv4 a IPv6 v příkazu ALTER QMGR IPADDRV. Není-li nastavena, předpokládá se "MQIPADDR_IPv4".

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- ProWindows:

```
SET MQIPADDRV=MQIPADDR_IPv4|MQIPADDR_IPv6
```

- Pro systémy SYSTÉM UNIX a Linux :

```
export MQIPADDRV=MQIPADDR_IPv4|MQIPADDR_IPv6
```

-  ProIBM i:

```
ADDENVVAR ENVVAR(MQIPADDRV) VALUE(MQIPADDR_IPv4|MQIPADDR_IPv6)
```

NÁZEV MQNAME

Parametr MQNAME určuje lokální název NetBIOS , který mohou procesy IBM MQ používat.

Úplný popis a pravidla priority na klientovi a na serveru viz [“Definování připojení NetBIOS v systému Windows”](#) na stránce 187 .

Chcete-li nastavit tuto proměnnou, použijte tento příkaz:

```
SET MQNAME=Your_env_Name
```

Příklad:

```
SET MQNAME=CLIENT1
```

NetBIOS na některých platformách vyžaduje pro každou aplikaci jiný název (nastavený pomocí MQNAME), pokud spouštíte více aplikací produktu IBM MQ zároveň na serveru IBM MQ MQI client.

SERVER MQSERVER

Proměnná prostředí MQSERVER se používá k definování minimálního kanálu. Parametr MQSERVER určuje umístění serveru IBM MQ a komunikační metodu, která má být použita.

Modul MQSERVER nelze použít k definování kanálu SSL nebo kanálu s uživatelskými procedurami kanálu. Podrobnosti o tom, jak definovat kanál SSL, najdete v tématu [Ochrana kanálů pomocí SSL](#).

ConnectionName musí být plně kvalifikovaný název sítě. Objekt *ChannelName* nesmí obsahovat znak lomítka (/), protože tento znak se používá k oddělení názvu kanálu, typu transportu a názvu připojení. Je-li pro definování kanálu klienta použita proměnná prostředí MQSERVER, bude použita maximální délka zprávy (MAXMSGL) o hodnotě 100 MB. Proto maximální velikost zprávy platná pro kanál je hodnota zadaná v kanálu SVRCONN na serveru.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- ProWindows:

```
SET MQSERVER=ChannelName/TransportType/ConnectionName
```

- Pro systémy SYSTÉM UNIX a Linux :

```
export MQSERVER='ChannelName/TransportType/ConnectionName'
```

-  ProIBM i:

```
ADDENVVAR ENVVAR(MQSERVER) VALUE('ChannelName/TransportType/ConnectionName')
```

-  Proz/OS

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/AMACHINE.ACOMPANY.COM(1414) '
```

TransportType může mít jednu z následujících hodnot, v závislosti na platformě klienta IBM MQ :

- LU62
- TCP
- NETBIOS
- SPX

ConnectionName může být čárkami oddělený seznam názvů připojení. Názvy připojení v seznamu se používají podobným způsobem jako více připojení v tabulce připojení klienta. Seznam *ConnectionName* může být použit jako alternativa pro skupiny správců front, aby bylo možné určit více připojení pro klienta, který se má pokusit. Pokud konfiguruje správce front s více instancemi, můžete použít seznam *ConnectionName* k určení různých instancí správce front.

Předvolený port TCP/IP

Při výchozím nastavení pro protokol TCP/IP produkt IBM MQ předpokládá, že kanál bude připojen k portu 1414.

Tento stav můžete změnit takto:

- Přidání čísla portu v hranatých závorkách jako poslední části pole *ConnectionName*:
 - Pro Windows:

```
SET MQSERVER=ChannelName/TransportType/ConnectionName(PortNumber)
```

- Pro systémy SYSTÉM UNIX a Linux :

```
export MQSERVER='ChannelName/TransportType/ConnectionName(PortNumber) '
```

- Změna souboru `mqclient.ini` přidáním čísla portu na název protokolu, například:

```
TCP:  
port=2001
```

- Přidejte IBM MQ do souboru služeb, jak je popsáno v tématu [“Použití modulu listener protokolu TCP/IP” na stránce 191](#).

Výchozí soket SPX

Při výchozím nastavení pro protokol SPX předpokládá produkt IBM MQ , že kanál bude připojen k soketu 5E86.

Tento stav můžete změnit takto:

- Přidání čísla soketu do hranatých závorek jako poslední části pole *ConnectionName*:

```
SET MQSERVER=ChannelName/TransportType/ConnectionName(SocketNumber)
```

U připojení SPX zadejte hodnotu *ConnectionName* a soket ve formě `network.node(socket)`. Pokud se klient a server IBM MQ nacházejí ve stejné síti, nemusí být tato síť zadána. Pokud používáte výchozí soket, nemusí být určen soket.

- Změna souboru `qm.ini` přidáním čísla portu na název protokolu, například:

```
SPX:  
socket=5E87
```

Použití produktu MQSERVER

Pokud používáte proměnnou prostředí MQSERVER k definování kanálu mezi počítačem se serverem IBM MQ MQI client a počítačem serveru, je tento kanál k dispozici pouze pro danou aplikaci a pro tabulku definic kanálů klienta (CCDT) není zadán žádný odkaz.

V této situaci program modulu listener, který jste spustili na počítači serveru, určuje správce front, k němuž se vaše aplikace připojí. Bude to stejný správce front, ke kterému je připojen program modulu listener.

Pokud požadavek MQCONN nebo MQCONNX určuje jiného správce front, než je modul listener, k němuž je připojen modul listener, nebo pokud parametr MQSERVER *TransportType* není rozpoznán, požadavek MQCONN nebo MQCONNX selže s návratovým kódem MQRC_Q_MGR_NAME_ERROR.

V systému SYSTÉM UNIX a Linux můžete definovat MQSERVER jako v jednom z následujících příkladů:

```
export MQSERVER=CHANNEL1/TCP/'9.20.4.56(2002)'  
export MQSERVER=CHANNEL1/LU62/BOX99
```

Všechny požadavky MQCONN nebo MQCONNX se pak pokusí použít kanál, který jste definovali, pokud na strukturu MQCD není odkazováno ze struktury MQCNO dodané s produktem MQCONNX. Kanál určený strukturou MQCD má v takovém případě přednost před danou strukturou prostředí MQSERVER.

Proměnná prostředí MQSERVER má přednost před všemi definicemi kanálů klienta, na které odkazuje MQCHLLIB a MQCHLTAB.

Rušení MQSERVER

Chcete-li zrušit volání MQSERVER a vrátit se do tabulky definic kanálů klienta, na kterou odkazuje proměnná MQCHLLIB a MQCHLTAB, zadejte následující příkaz:

- zapWindows:

```
SET MQSERVER=
```

- V systémech SYSTÉM UNIX a Linux:

```
unset MQSERVER
```

MQSSLCRYP

Funkce MQSSLCRYP obsahuje řetězec parametrů, který vám umožňuje konfigurovat kryptografický hardware přítomný v systému. Povolené hodnoty jsou stejné jako u parametru **SSLCRYP** příkazu **ALTER QMGR**.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Na systémech Windows:

```
SET MQSSLCRYP=string
```

- Na systémech SYSTÉM UNIX a Linux:

```
export MQSSLCRYP=string
```

Související informace

Parametr **ALTER QMGR** příkazu **SSLCRYP**

MQSSLFIPS

Hodnota MQSSLFIPS určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, je-li šifrování prováděno v produktu IBM MQ. Hodnoty jsou stejné jako u parametru SSLFIPS příkazu ALTER QMGR.

Použití algoritmů certifikovaných FIPS je ovlivněno používáním kryptografického hardwaru, viz [Určení, že se v klientu MQI používá pouze certifikovaný standard FIPS CipherSpecs](#).

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Na systémech Windows:

```
SET MQSSLFIPS=YES|NO
```

- Na systémech SYSTÉM UNIX a Linux:

```
export MQSSLFIPS=YES|NO
```

-  IBM i zapIBM i:

```
ADDENVVAR ENVVAR(MQSSLFIPS) VALUE(YES|NO)
```

Výchozí hodnota je NO.

MQSSLKEYR

MQSSLKEYR určuje umístění úložiště klíčů, které uchovává digitální certifikát patřící uživateli, v kmenového formátu. Formát Stem znamená, že obsahuje úplnou cestu a název souboru bez přípony.

Podrobné informace naleznete v parametru [SSLKEYR](#) příkazu ALTER QMGR.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Na systémech Windows:

```
SET MQSSLKEYR=pathname
```

- Na systémech SYSTÉM UNIX a Linux:

```
export MQSSLKEYR=pathname
```

-  IBM i zapIBM i:

```
ADDENVVAR ENVVAR(MQSSLKEYR) VALUE(pathname)
```

Není zde žádná výchozí hodnota.

MQSSLPROXY

Hodnota MQSSLPROXY určuje název hostitele a číslo portu serveru proxy HTTP, který má sada GSKit použít pro kontroly OCSP.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Na systémech Windows:

```
SET MQSSLPROXY= string
```

- Na systémech SYSTÉM UNIX a Linux:

```
export MQSSLPROXY="string"
```

Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použít pro kontroly OCSP. Za touto adresou může následovat volitelné číslo portu uzavřené v závorkách. Pokud číslo portu neurčíte, zvolí se výchozí port HTTP, který má číslo 80.

Například v systémech SYSTÉM UNIX a Linux můžete použít jeden z následujících příkazů:

- ```
export MQSSLPROXY="proxy.example.com(80)"
```
- ```
export MQSSLPROXY="127.0.0.1"
```

MQSSLRESET

Hodnota MQSSLRESET představuje počet nezašifrovaných bajtů odeslaných a přijatých v rámci kanálu SSL nebo TLS před opětovným získáním tajného klíče.

Další informace o novém domlouvání klíče najdete v tématu [Reset tajných klíčů SSL a TLS](#).

Může být nastavena na celé číslo v rozsahu od 0 do 999 999 999. Výchozí hodnota je 0, což znamená, že tajné klíče nejsou nikdy znovu vyjednávány. Pokud zadáte počet obnovení tajných klíčů zabezpečení SSL nebo TLS v rozsahu od 1 bajtu do 32 KB, budou kanály zabezpečení SSL nebo TLS používat počet obnovení tajných klíčů 32 kB. Tento počet obnovení utajení je, aby se zabránilo nadměrnému resetování klíčů, které by mohlo nastat pro malé hodnoty resetování tajného klíče SSL nebo TLS.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Na systémech Windows:

```
SET MQSSLRESET=integer
```

- Na systémech SYSTÉM UNIX a Linux:

```
export MQSSLRESET=integer
```

-  zapIBM i:

```
ADDENVVAR ENVVAR(MQSSLRESET) VALUE(integer)
```

MQSUITEB.

Produkt IBM MQ můžete nakonfigurovat tak, aby pracoval v souladu s normou NSA Suite B na platformách Windows, SYSTÉM UNIX a Linux.

Sada B omezuje sadu povolených šifrovacích algoritmů tak, aby byla zajištěna zajištěná úroveň zabezpečení.

Další informace viz [Konfigurace produktu IBM MQ for Suite B](#).

MQTCPTIMEOUT

Jak dlouho IBM MQ čeká na volání spojení TCP.

Změna konfiguračních informací IBM MQ a správce front

Změňte chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Informace o konfiguraci produktu IBM MQ můžete změnit tak, že změníte hodnoty zadané na sadě konfiguračních atributů (nebo parametrů), které řídí IBM MQ.

Změňte informace o atributu upravením konfiguračních souborů IBM MQ . V systémech IBM MQ for Windows a Linux (platformy x86 a x86-64) lze konfigurační soubory produktu IBM MQ upravovat pomocí produktu MQ Explorer.

Na systémech Windows můžete také použít amqmdain pro změnu konfiguračních informací, jak je popsáno v [amqmdain](#)

Další informace o konfiguraci produktu IBM MQ a správců front pro danou platformu naleznete v následujících dílčích tématech:

Související pojmy

[“Konfigurace” na stránce 5](#)

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

[“Konfigurace správců front v systému z/OS” na stránce 523](#)

Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Související informace

[Naplánování](#)

[Správa serveru IBM MQ](#)

Změna konfiguračních informací v systémech Windows, SYSTÉM UNIX a Linux

Konfigurační atributy se nacházejí v konfiguračních souborech, na úrovni uzlu a správce front.

Na platformách Windows, SYSTÉM UNIX a Linux můžete změnit atributy konfigurace produktu IBM MQ v rámci následujících položek:

- Konfigurační soubor IBM MQ (**mqs.ini**). aby se projevil změny pro IBM MQ na uzlu jako celku. Pro každý uzel je k dispozici jeden soubor mqs.ini .

Další informace o stanzách uvedených v souboru **mqs.ini** naleznete v tématu [“Atributy pro změnu konfiguračních informací IBM MQ” na stránce 98](#) .

- Konfigurační soubor správce front (**qm.ini**) ovlivní změny pro specifické správce front. Pro každého správce front v daném uzlu existuje jeden soubor qm.ini .

Další informace o stanzách uvedených v souboru **qm.ini** naleznete v tématu [“Změna konfiguračních informací správce front” na stránce 105](#) .

Volby konfigurace klienta jsou drženy odděleně v konfiguračním souboru klienta.

Konfigurační soubor (nebo soubor **stanza**) obsahuje jednu nebo více oddílů, které jsou skupinami linek v souboru .ini, které mají společnou funkci nebo definují část systému, jako jsou funkce protokolování, funkce kanálů a instalovatelné služby.

Protože konfigurační soubor produktu IBM MQ se používá k vyhledání dat přidružených ke správcům front, může neexistující nebo chybný konfigurační soubor způsobit selhání některých nebo všech příkazů MQSC. Aplikace se také nemohou připojit ke správci front, který není definován v konfiguračním souboru IBM MQ .

Jakékoli změny, které provedete v konfiguračním souboru, se obvykle projeví až po příštím spuštění správce front.

V systémech Windows a Linux (platformy x86 a x86-64) můžete upravit informace o konfiguraci ze serveru MQ Explorer.

Na systémech Windows můžete také použít příkaz `amqmdain` k úpravě konfiguračních souborů.

Další informace o volbách konfigurace v systémech Windows, SYSTÉM UNIX a Linux najdete v následujících dílčích tématech:

Související pojmy

[“Konfigurace” na stránce 5](#)

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

[“Změna konfiguračních informací IBM MQ a správce front” na stránce 81](#)

Změňte chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související odkazy

[“Změna konfiguračních informací v systému IBM i” na stránce 87](#)

V této části se dozvíte, jak změnit chování správců front tak, aby vyhovovaly potřebám vaší instalace.

[“Atributy pro změnu konfiguračních informací IBM MQ” na stránce 98](#)

V systémech IBM MQ for Windows a v systémech IBM MQ for Linux (platformy x86 a x86-64) upravte konfigurační informace pomocí Průzkumníka IBM MQ. V jiných systémech upravte informace úpravou konfiguračního souboru `mqs.ini`.

[“Změna konfiguračních informací správce front” na stránce 105](#)

Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro IBM MQ.

Související informace

[Naplánování](#)

[Správa serveru IBM MQ](#)

Úprava konfiguračních souborů

Úprava konfiguračních souborů pomocí příkazů nebo standardního textového editoru.

Před úpravou konfiguračního souboru jej zálohujte tak, abyste měli kopii, na kterou se můžete vrátit, pokud k tomu dojde.

Konfigurační soubory můžete upravit buď:

- Automaticky pomocí příkazů, které mění konfiguraci správců front v uzlu
- Ruční při použití standardního textového editoru

Po instalaci můžete upravit výchozí hodnoty v konfiguračních souborech produktu IBM MQ.

Pokud jste v atributu konfiguračního souboru nastavili nesprávnou hodnotu, hodnota se ignoruje a vydá se zpráva operátora, která daný problém označuje. (Efekt je stejný jako chybějící atribut zcela.)

Při vytváření nového správce front postupujte takto:

- Zazálohujte konfigurační soubor IBM MQ
- Vytvořte zálohu nového konfiguračního souboru správce front

Komentáře mohou být zahrnuty do konfiguračních souborů přidáním znaku ";" nebo znaku "#" před text komentáře. Chcete-li použít znak ";" nebo "#" bez reprezentace komentáře, můžete před znakem zadat znak "\" a tento znak se bude používat jako součást konfiguračních dat.

Kdy je třeba upravit konfigurační soubor?

Upravte konfigurační soubor tak, aby se zotavilo ze zálohy, přesuňte správce front, změňte výchozího správce front nebo asistujte podporu produktu IBM.

Možná budete muset upravit konfigurační soubor, pokud například:

- Ztratíte konfigurační soubor. (Obnova ze zálohy, pokud můžete.)
- Je třeba přesunout jednoho nebo více správců front do nového adresáře.

- Pokud omylem odstraníte existujícího správce front, je třeba změnit výchozího správce front.
- Je vám doporučeno, abyste to udělali pomocí svého střediska podpory produktu IBM .

Priority konfiguračního souboru

Hodnota atributu je definována na více místech. Atributy nastavené v příkazech mají přednost před atributy v konfiguračních souborech.

Hodnoty atributu konfiguračního souboru jsou nastaveny podle následujících priorit:

- Parametry zadané na příkazovém řádku mají přednost před hodnotami definovanými v konfiguračních souborech
- Hodnoty definované v souborech qm.ini mají přednost před hodnotami definovanými v souboru mqs.ini .

Konfigurační soubor IBM MQ , mqs.ini .

Konfigurační soubor IBM MQ mqs.iniobsahuje informace vztahující se ke všem správcům front v daném uzlu. Vytvoří se automaticky během instalace.

V produktech IBM MQ for UNIX a Linux jsou datový adresář a adresář protokolu vždy /var/mqm a /var/mqm/log .

V systémech Windows jsou umístění datového adresáře mqs . inia umístění adresáře protokolu uloženy v registru, protože jejich umístění se může lišit.

Kromě toho se v systémech Windows nachází v registru informace o konfiguraci instalace (obsažené v produktu mqinst . ini v systémech IBM MQ for UNIXa Linux), protože v produktu Windowsnení k dispozici žádný soubor mqinst . ini .

Soubor mqs.ini pro systémy Windows je dán parametrem WorkPath uvedeným v klíči HKLM\SOFTWARE\IBM\WebSphere MQ . Obsahuje:

- Názvy správců front
- Název výchozího správce front
- Umístění souborů přidružených ke každému z nich

Dodaná sekce LogDefault s pro novou instalaci IBM MQ neobsahuje žádné explicitní hodnoty pro atributy. Chybějící atribut znamená, že výchozí hodnota pro tuto hodnotu se používá při vytvoření nového správce front. Standardní hodnoty jsou zobrazeny pro stanzu LogDefault s v Obrázek 5 na stránce 84. Hodnota nula pro atribut LogBufferPages znamená 512.

Pokud požadujete jinou než výchozí hodnotu, musíte tuto hodnotu explicitně zadat ve stanze LogDefault s .

```

#*****#
#* Module Name: mqs.ini                                     *#
#* Type       : IBM MQ Machine-wide Configuration File     *#
#* Function   : Define IBM MQ resources for an entire machine *#
#*****#
#* Notes     :                                             *#
#* 1) This is the installation time default configuration *#
#*                                                  *#
#*****#
AllQueueManagers:
#*****#
#* The path to the qmgrs directory, below which queue manager data *#
#* is stored                                                         *#
#*****#
DefaultPrefix=/var/mqm

LogDefaults:
  LogPrimaryFiles=3
  LogSecondaryFiles=2
  LogFilePages=4096
  LogType=CIRCULAR
  LogBufferPages=0
  LogDefaultPath=/var/mqm/log

QueueManager:
  Name=saturn.queue.manager
  Prefix=/var/mqm
  Directory=saturn!queue!manager
  InstallationName=Installation1

QueueManager:
  Name=pluto.queue.manager
  Prefix=/var/mqm
  Directory=pluto!queue!manager
  InstallationName=Installation2

DefaultQueueManager:
  Name=saturn.queue.manager

ApiExitTemplate:
  Name=OurPayrollQueueAuditor
  Sequence=2
  Function=EntryPoint
  Module=/usr/ABC/auditor
  Data=123

ApiExitCommon:
  Name=MQPoliceman
  Sequence=1
  Function=EntryPoint
  Module=/usr/MQPolice/tmqp
  Data=CheckEverything

```

Obrázek 5. Příklad konfiguračního souboru IBM MQ pro Systémy SYSTÉM UNIX

Konfigurační soubory správce front qm.ini

Konfigurační soubor správce front `qm.ini` obsahuje informace vztahující se ke specifickému správci front.

Pro každého správce front existuje jeden konfigurační soubor správce front. Soubor `qm.ini` je automaticky vytvořen při vytvoření správce front, se kterým je asociován.

V 8.0.0.8 V produktu IBM MQ 8.0.0, opravná sada Fix Pack 8příkaz **strmqm** kontroluje syntaxi oddílů CHANNELS a SSL v souboru `qm.ini` před úplným spuštěním správce front, takže je mnohem snazší zjistit, co je špatně, a správně ji opravte, pokud **strmqm** zjistí, že soubor `qm.ini` obsahuje chyby. Další informace viz [strmqm](#).

Umístění souborů qm.ini

V systémech SYSTÉM UNIX a Linux se soubor qm.ini nachází v kořenovém adresáři adresářového stromu obsazené správcem front. Příklad: Cesta a název konfiguračního souboru pro správce front s názvem QMNAME je:

```
/var/mqm/qmgrs/QMNAME/qm.ini
```

Na systémech Windows je umístění souboru qm.ini dáno parametrem WorkPath zadaným v klíči HKLM\SOFTWARE\IBM\WebSphere MQ. Příklad: Cesta a název konfiguračního souboru pro správce front s názvem QMNAME je:

```
C:\ProgramData\IBM\MQ\qmgrs\QMNAME\qm.ini
```

Název správce front může mít délku až 48 znaků. To však nezaručuje, že název je platný nebo jedinečný. Proto je název adresáře generován na základě názvu správce front. Tento proces je znám jako *transformace názvu*. Popis naleznete v tématu [Základní informace o názvech souborů produktu IBM MQ](#).

Příklad souboru qm.ini

Linux UNIX

Následující příklad ukazuje, jak mohou být skupiny atributů uspořádány v konfiguračním souboru správce front v systémech IBM MQ for UNIX a Linux .

```
##* Module Name: qm.ini                                *##
##* Type       : IBM MQ queue manager configuration file *##
##* Function   : Define the configuration of a single queue manager *##
##*           *##
##*****#
##* Notes     : *##
##* 1) This file defines the configuration of the queue manager *##
##*           *##
##*****#

ExitPath:
  ExitsDefaultPath=/var/mqm/exits
  ExitsDefaultPath64=/var/mqm/exits64

Service:
  Name=AuthorizationService
  EntryPoints=14

ServiceComponent:
  Service=AuthorizationService
  Name=MQSeries.UNIX.auth.service
  Module=amqzfu
  ComponentDataSize=0

Log:
  LogPrimaryFiles=3
  LogSecondaryFiles=2
  LogFilePages=4096
  LogType=CIRCULAR
  LogBufferPages=0 1
  LogPath=/var/mqm/log/saturn!queue!manager/

XAResourceManager:
  Name=DB2 Resource Manager Bank
  SwitchFile=/usr/bin/db2swit
  XAOpenString=MQBankDB
  XACloseString=
  ThreadOfControl=THREAD

Channels: 2
  MaxChannels=200
  MaxActiveChannels=100
  MQIBindType=STANDARD

TCP:
  SndBuffSize=0
```

```
RcvBuffSize=0
RcvSndBuffSize=0
RcvRcvBuffSize=0
ClntSndBuffSize=0
ClntRcvBuffSize=0
SvrSndBuffSize=0
SvrRcvBuffSize=0
```

```
QMErrorLog:
  ErrorLogSize=262144
  ExcludeMessage=7234
  SuppressMessage=9001,9002,9202
  SuppressInterval=30
```

```
ApiExitLocal:
  Name=ClientApplicationAPIChecker
  Sequence=3
  Function=EntryPoint
  Module=/usr/Dev/ClientAppChecker
  Data=9.20.176.20
```

Všimněte si, že soubor `qm.ini` pro Windows obsahuje další stanzu `AccessMode` :

```
AccessMode:
  SecurityGroup=wmq\wmq
```

Notes:

1. Hodnota nula pro `LogBufferPages` udává hodnotu 512.
2. Další informace o sekci Kanál naleznete v tématu [“Inicializační a konfigurační soubory”](#) na stránce 169.
3. Maximální počet oddílů `XAResourceManager` je omezen na 255. Měli byste však použít pouze malý počet oddílů, abyste se vyvarovali snížení výkonu transakce.
4. **distributed** From IBM MQ 8.0, for new queue managers on distributed platforms, the default TCP send and receive buffer sizes in the TCP stanza of the `qm.ini` file are set to be managed by the operating system. Noví správci front jsou automaticky vytvářeni s následujícími výchozími nastaveními pro vyrovnávací paměti pro odesílání a příjem:

```
TCP:
  SndBuffSize=0
  RcvBuffSize=0
  RcvSndBuffSize=0
  RcvRcvBuffSize=0
  ClntSndBuffSize=0
  ClntRcvBuffSize=0
  SvrsndBuffSize=0
  SvrrcvBuffSize=0
```

Před Verze 8.0, bez ručního ladění, jsou tyto hodnoty standardně nastaveny na pevnou velikost 32Kb .

Tato změna platí pouze pro nové správce front. Nastavení vyrovnávací paměti pro odeslání a příjem TCP pro správce front, kteří jsou migrováni z dřívějších vydání, je zachován.

Informace o tom, jak ručně nastavit velikosti vyrovnávací paměti TCP pro použití výchozího chování operačního systému pro migrované správce front, najdete v tématu [TCP, LU62, NETBIOS a SPX](#).

Informace o tom, kdy se změny projeví, naleznete v příručce [“Změna konfiguračních informací v systémech Windows, SYSTÉM UNIX a Linux”](#) na stránce 81 .

Související odkazy

[“TCP, LU62a NETBIOS”](#) na stránce 115

Chcete-li zadat parametry konfigurace síťového protokolu, použijte tyto stránky vlastností správce front nebo oddíly v souboru `qm.ini` . Přepisují výchozí atributy pro kanály.

Konfigurační soubor instalace mqinst.ini

Systemy SYSTÉM UNIX a Linux

Konfigurační soubor instalace mqinst.ini obsahuje informace o všech instalacích produktu IBM MQ v systému UNIX nebo Linux .

Soubor mqinst.ini se nachází v adresáři /etc/opt/mqm na systémech SYSTÉM UNIX a Linux . Obsahuje informace o instalaci, je-li k dispozici, o primární instalaci a o následujících informacích pro každou instalaci:

- Název instalace
- Popis instalace
- Identifikátor instalace
- Instalační cesta

Tento soubor nesmí být upravován nebo odkazován přímo, protože jeho formát není pevný a mohl by se změnit. Místo toho použijte následující příkazy k vytvoření, odstranění, dotazu a úpravě, hodnot v souboru mqinst.ini :

[crtmqinst](#) pro vytvoření položek.
[dlmqinst](#) k odstranění položek.
[dspmqinst](#) pro zobrazení položek.
[setmqinst](#) pro nastavení položek.

Je automaticky nastaven identifikátor instalace, pouze pro vnitřní použití, a nesmí být změněn.

Systemy Windows

Informace o konfiguraci instalace jsou uloženy v následujícím klíči na systémech Windows :

```
HKLM\SOFTWARE\IBM\WebSphere MQ\Installation\
```

Tento klíč nesmí být upravován nebo odkazován přímo, protože jeho formát není pevný a mohl by se změnit. Místo toho použijte následující příkazy k dotazování a úpravě hodnot v registru:

[dspmqinst](#) pro zobrazení položek.
[setmqinst](#) pro nastavení položek.

V systému Windows jsou k dispozici příkazy **crtmqinst** a **dlmqinst** . Procesy instalace a odinstalace manipulují s vytvářením a odstraňováním požadovaných položek registru.

Změna konfiguračních informací v systému IBM i

V této části se dozvíte, jak změnit chování správců front tak, aby vyhovovaly potřebám vaší instalace.

Informace o konfiguraci produktu IBM MQ změníte tím, že upravíte hodnoty zadané na sadě konfiguračních atributů (nebo parametrů), které řídí IBM MQ. Tyto atributy změníte upravením konfiguračních souborů **IBM MQ**.

Informace o úpravách konfiguračních hodnot v systému IBM najdete v následujících tématech:

- [“IBM MQ for IBM i Konfigurační soubory”](#) na stránce 88
- [“Atributy pro změnu konfiguračních informací IBM MQ for IBM i”](#) na stránce 89
- [“Změna konfiguračních informací správce front IBM MQ”](#) na stránce 92
- [“Příklad souborů IBM i mq5.ini a qm.ini”](#) na stránce 96

Související pojmy

[“Konfigurace”](#) na stránce 5

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

[“Změna konfiguračních informací IBM MQ a správce front” na stránce 81](#)

Změňte chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

[“Změna konfiguračních informací v systémech Windows, SYSTÉM UNIX a Linux” na stránce 81](#)

Konfigurační atributy se nacházejí v konfiguračních souborech, na úrovni uzlu a správce front.

Související odkazy

[“Atributy pro změnu konfiguračních informací IBM MQ” na stránce 98](#)

V systémech IBM MQ for Windows a v systémech IBM MQ for Linux (platformy x86 a x86-64) upravte konfigurační informace pomocí Průzkumníka IBM MQ. V jiných systémech upravte informace úpravou konfiguračního souboru mqs.ini.

[“Změna konfiguračních informací správce front” na stránce 105](#)

Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro IBM MQ.

Související informace

[Naplánování](#)

[Správa serveru IBM MQ](#)

IBM MQ for IBM i Konfigurační soubory

Tyto informace vám pomohou pochopit metody konfigurace produktu IBM MQ for IBM i.

Konfigurační atributy produktu IBM MQ upravujete v rámci:

- Konfigurační soubor IBM MQ, mqs.ini, ovlivňují změny na uzlu jako celku. Pro každou instalaci produktu IBM MQ je k dispozici jeden soubor mqs.ini.
- Konfigurační soubor správce front qm.ini, provedení změn pro specifické správce front. Pro každého správce front v daném uzlu existuje jeden soubor qm.ini.

Všimněte si, že soubory .ini jsou proudovými soubory, které jsou rezidentní v IFS.

Konfigurační soubor (který může být označován jako soubor **stanza**) obsahuje jednu nebo více oddílů, které jsou skupinami linek v souboru .ini, které mají společnou funkci nebo definují část systému, například funkce protokolů a funkce kanálů. Všechny změny provedené v konfiguračním souboru se projeví až po příštím spuštění správce front.

Úprava konfiguračních souborů

Před úpravou konfiguračního souboru jej zálohujte tak, abyste měli kopii, na kterou se můžete vrátit, pokud k tomu dojde.

Konfigurační soubory můžete upravit buď:

- Automaticky pomocí příkazů, které mění konfiguraci správců front v uzlu.
- Ručně, pomocí editoru jazyka CL EDTF.

Po instalaci můžete upravit výchozí hodnoty v konfiguračních souborech produktu IBM MQ. Pokud jste v atributu konfiguračního souboru nastavili nesprávnou hodnotu, hodnota se ignoruje a vydá se zpráva operátora, která daný problém označuje. (Efekt je stejný jako chybějící atribut zcela.)

Při vytváření nového správce front postupujte takto:

- Zazálohujte konfigurační soubor IBM MQ.
- Vytvořte zálohu nového konfiguračního souboru správce front.

Kdy je třeba upravit konfigurační soubor?

Možná budete muset upravit konfigurační soubor, pokud například:

- Ztratíte konfigurační soubor; pokud je to možné, obnovte jej ze zálohy.
- Je třeba přesunout jednoho nebo více správců front do nového adresáře.
- Pokud omylem odstraníte existujícího správce front, je třeba změnit výchozího správce front.
- Je vám doporučeno, abyste to udělali pomocí svého střediska podpory produktu IBM .

Priority konfiguračního souboru

Hodnoty atributu konfiguračního souboru jsou nastaveny podle následujících priorit:

- Parametry zadané na příkazovém řádku mají přednost před hodnotami definovanými v konfiguračních souborech.
- Hodnoty definované v souborech `qm.ini` mají přednost před hodnotami definovanými v souboru `mqs.ini`.

Konfigurační soubor IBM MQ `mqs.ini`

Konfigurační soubor IBM MQ , `mqs.ini`, obsahuje informace vztahující se ke všem správcům front v instalaci produktu IBM MQ . Vytvoří se automaticky během instalace. Konkrétně se používá soubor `mqs.ini` k vyhledání dat přidružených ke každému správci front.

Soubor `mqs.ini` je uložen v adresáři `/QIBM/UserData/mqm`

Soubor `mqs.ini` obsahuje:

- Názvy správců front.
- Název výchozího správce front.
- Umístění souborů přidružených ke každému správci front.
- Informace identifikující jakékoli uživatelské procedury rozhraní API (viz [Konfigurace uživatelských procedur rozhraní API](#) , kde získáte další informace).

Konfigurační soubory správce front `qm.ini`

Konfigurační soubor správce front `qm.ini` obsahuje informace vztahující se ke specifickému správci front. Pro každého správce front existuje jeden konfigurační soubor správce front. Soubor `qm.ini` se vytvoří automaticky, když je vytvořen správce front, se kterým je asociován.

Soubor `qm.ini` se nachází v souboru `<mqmdata directory>/QMNAME/qm.ini`, kde `<mqmdata directory>` je standardně `/QIBM/UserData/mqm` a `QMNAME` je název správce front, pro kterého se použije inicializační soubor.

Poznámka:

1. Můžete změnit `<mqmdata directory>` v souboru `mqs.ini`.
2. Název správce front může mít délku až 48 znaků. To však nezaručuje, že název je platný nebo jedinečný. Proto je název adresáře generován na základě názvu správce front. Tento proces je znám jako **transformace názvu**. Další informace viz [Základní informace o názvech knihoven správce front produktu IBM MQ for IBM i](#).

Atributy pro změnu konfiguračních informací IBM MQ for IBM i

Tyto informace vám pomohou pochopit sekce s informacemi o konfiguraci.

V produktu `mqs.ini` se vyskytují tyto skupiny atributů:

- [“Sekce Manažeři AllQueue” na stránce 90](#)
- [“Sekce správce DefaultQueueManager” na stránce 91](#)
- [“Sekce ExitProperties” na stránce 91](#)
- [“Sekce QueueManager” na stránce 92](#)

Existují také dvě stanzy přidružené k uživatelským procedurám API, `ApiExitCommon` a `ApiExitTemplate`. Podrobnosti o použití těchto viz téma [Konfigurace uživatelských procedur rozhraní API](#).

Sekce Manažeři AllQueue

Stanza `AllQueueManagers` může uvádět:

- Cesta k adresáři `qmgrs`, kde jsou uloženy soubory přidružené ke správci front
- Cesta ke spustitelné knihovně
- Metoda pro převod dat ve formátu EBCDIC do formátu ASCII

V popisech oddílů je podtržená hodnota výchozí hodnotou a | symbol znamená *nebo*.

DefaultPrefix= *název_adresáře*

Cesta k adresáři `qmgrs`, v němž jsou uložena data správce front. Pokud změníte výchozí předponu pro správce front, musíte replikovat strukturu adresáře, která byla vytvořena při instalaci. Konkrétně musíte vytvořit strukturu `qmgrs`. Před změnou výchozí předpony ukončete produkt IBM MQ a znovu spusťte produkt IBM MQ pouze po přesunutí struktur do nového umístění a změně výchozí předpony.

Jako alternativu ke změně výchozí předpony můžete použít proměnnou prostředí `MQSPREFIX` k potlačení `DefaultPrefix` pro příkaz `CRTMQM`.

ConvEBCDICNewline= NL_TO_LF | TABLE | ISO

Kódové stránky EBCDIC obsahují znak nového řádku (NL), který není podporován kódovými stránkami ASCII, ačkoli některé varianty ISO ASCII obsahují ekvivalent.

Použijte atribut `ConvEBCDICNewline` k uvedení metody IBM MQ, která se má použít při konverzi znaku NL EBCDIC na formát ASCII.

NL_TO_LF

Konvertuje znak NL (X'15 ') EBCDIC na znak LF (X'0A'), pro všechny převody z formátu EBCDIC na ASCII.

Výchozí hodnota `NL_TO_LF` je výchozí.

TABULKA

Převedte znak NL kódové stránky EBCDIC podle převodních tabulek používaných v systému IBM i pro všechny převody z formátu EBCDIC na ASCII.

Všimněte si, že vliv tohoto typu převodu se může lišit od jazyka do jazyka.

ISO

Uved'te ISO, pokud chcete:

- CCSID ISO, které mají být převedeny pomocí metody `TABLE`
- Všechny ostatní CCSID, které se mají konvertovat pomocí metody `NL_TO_CF`.

Možné identifikátory CCSID ISO jsou zobrazeny v [Tabulka 11](#) na stránce 90.

<i>Tabulka 11. Seznam možných ISO CCSID</i>	
CCSID	Kódová sada
819	ISO8859-1
912	ISO8859-2
915	ISO8859-5
1089	ISO8859-6
813	ISO8859-7
916	ISO8859-8

Tabulka 11. Seznam možných ISO CCSID (pokračování)	
CCSID	Kódová sada
920	ISO8859-9
1051	roman8

Není-li ASCII CCSID podmnožinou ISO, ConvEBCDICNewline standardně zobrazuje NL_TO_LF.

Sekce správce DefaultQueueManager

Stanza DefaultQueueManager určuje výchozího správce front pro uzel.

Název = výchozí_správce_front

Výchozí správce front zpracovává všechny příkazy, pro které není explicitně určen název správce front. Atribut DefaultQueueManager se automaticky aktualizuje, pokud vytvoříte nového výchozího správce front. Pokud jste neúmyslně vytvořili nového výchozího správce front a poté se chcete vrátit k původnímu správci front, musíte atribut DefaultQueueManager změnit ručně.

Sekce ExitProperties

Stanza ExitProperties uvádí volby konfigurace používané ukončovacími programy správce front.

V popisech oddílů je podtržená hodnota výchozí hodnotou a | symbol znamená *nebo*.

CLWLMode= SAFE | FAST

Uživatelská procedura pracovní zátěže klastru CLWL vám umožňuje určit, která fronta klastru v klastru má být otevřena v rámci odezvy na volání MQI (například MQOPEN nebo MQPUT). Uživatelská procedura CLWL se spustí buď v režimu FAST, nebo v režimu SAFE, v závislosti na hodnotě, kterou zadáte v atributu CLWLMode. Pokud vynecháte atribut CLWLMode, uživatelská procedura pracovní zátěže klastru se spustí v režimu SAFE.

SAFE

Spusťte uživatelskou proceduru CLWL v samostatném procesu pro správce front. Toto nastavení je výchozí.

Pokud se vyskytne problém s uživatelskou procedurou CLWL, když je spuštěn v režimu SAFE, nastane následující situace:

- Proces serveru CLWL (amqzlw0) selže
- Správce front restartuje proces serveru CLWL
- Chyba je ohlášena v protokolu chyb. Pokud probíhá volání MQI, obdržíte oznámení ve formě chybného návratového kódu.

Integrita správce front je zachována.

Poznámka: Spuštění uživatelské procedury CLWL v odděleném procesu může mít škodlivé účinky na výkon.

FAST

Spusťte uživatelskou proceduru klastru vloženou do procesu správce front.

Zadáním této volby zvýšíte výkon tím, že se vyhnete režii, která je přidružena ke spuštění v režimu SAFE, ale provádí se tak na úkor integrity správce front. Spusťte uživatelskou proceduru CLWL v režimu FAST pouze v případě, že jste přesvědčeni, že k ukončení CLWL nejsou žádné problémy **ne**, a vy jste obzvláště znepokojeni výkonnostními náklady.

Pokud se vyskytne problém, když je uživatelská procedura CLWL spuštěna v režimu FAST, správce front selže a vy spustíte riziko narušení integrity integrity správce front.

Sekce QueueManager

Pro každého správce front je zde jedna stanza `QueueManager`. Tyto atributy určují název správce front a název adresáře, který obsahuje soubory přidružené k tomuto správci front. Název adresáře je založen na názvu správce front, ale v případě, že název správce front není platným názvem souboru, je transformován.

Další informace o transformaci názvu viz [Základní informace o názvech knihoven správce front produktu IBM MQ for IBM i](#).

Název = `queue_manager_name`

Název správce front.

Předpona = `předpona`

Kde jsou uloženy soubory správce front. Ve výchozím nastavení je to stejné jako hodnota zadaná v atributu `DefaultPrefix` stanzy `AllQueueManager` v souboru `mqs.ini`.

Adresář = `název`

Název podadresáře pod adresářem `<prefix>\QMGRS`, kde jsou uloženy soubory správce front. Tento název je založen na názvu správce front, lze jej však transformovat, pokud existuje duplicitní název, nebo pokud název správce front není platným názvem souboru.

Knihovna = `název`

Název knihovny, do které jsou uloženy objekty produktu IBM i týkající se tohoto správce front, například žurnály a příjemce žurnálu. Tento název je založen na názvu správce front, lze jej však transformovat, pokud existuje duplicitní název, nebo pokud název správce front není platným názvem knihovny.

Změna konfiguračních informací správce front IBM MQ

Tyto informace vám pomohou porozumět stanzách konfigurace správce front.

Existují dvě stanzy přidružené k uživatelským procedurám `API`, `ApiExitCommon` a `ApiExitTemplate`. Podrobnosti o použití těchto viz téma [Konfigurace uživatelských procedur rozhraní API](#).

Následující skupiny atributů se mohou vyskytovat v souboru `qm.ini` pro specifického správce front nebo mohou být použity k přepsání hodnot nastavených v produktu `mqs.ini`.

Informace o změně informací o konfiguraci pro specifické volby naleznete v následujících tématech:

- [“Sekce Protokol” na stránce 92](#)
- [“Sekce Kanály” na stránce 93](#)
- [“stanza `QMErrorLog` na systému IBM i” na stránce 94](#)
- [“Sekce TCP” na stránce 95](#)
- [“stanza `PreConnect` konfiguračního souboru klienta” na stránce 65](#)

Sekce Protokol

Parametry pro konfiguraci souboru protokolu.

Stanza `Log` uvádí atributy protokolu pro určitého správce front. Při výchozím nastavení jsou tato nastavení zděděna z nastavení zadaného v sekci `LogDefaults` souboru `mqs.ini` při vytvoření správce front.

Změňte atributy této stanzy pouze v případě, že chcete konfigurovat správce front jinak než ostatní.

Hodnoty uvedené na attributech v souboru `qm.ini` se čtou, když je spuštěn správce front. Soubor je vytvořen při vytvoření správce front.

Velikost `LogBuffer`

Velikost vyrovnávací paměti žurnálu, v bajtech. Zadejte číslo v rozsahu 32 000 až 15 761 440. Výchozí hodnota je 32 000.

`LogPath`= `název_knihovny`

Název knihovny, která se používá k ukládání žurnálů a žurnálových zásobníků pro tohoto správce front.

Velikost LogReceiver

Velikost žurnálového zásobníku v kilobajtech. Výchozí hodnota je 100 000.

Sekce Kanály

Sekce Channels obsahuje informace o kanálech.

MaxChannels= **100** | číslo

Maximální povolený počet *aktuálních* kanálů. Pro z/OS musí být hodnota 1-9999, přičemž výchozí hodnota je 200. U všech ostatních platform musí být hodnota 1-65 535, přičemž výchozí hodnota je 100.

MaxActiveChannels = *hodnota MaxChannels_value*

Maximální počet kanálů povolených pro *aktivní* kdykoli. Předvolba je hodnota uvedená na atributu MaxChannels.

MaxInitiators= **3** | číslo

Maximální počet inicializátorů. Výchozí a současně maximální hodnota je 3.

MQIBINDTYPE=FASTPATH | STANDARD

Vazba pro aplikace.

Rychlý

Kanály se připojují pomocí struktury MQCONNX FASTPATH. To znamená, že neexistuje žádný proces agenta.

STANDARD

Kanály se připojují pomocí STANDARD.

ThreadedListener= **NO** | YES

Zda se má spustit RUNMQLSR (YES) nebo AMQCLMAA (NO) jako modul listener.

Uvedete-li ThreadedListener= ANO, všechny kanály se spustí jako vlákna jediné úlohy. Tím omezíte počet připojení k prostředkům, které jsou k dispozici pro jednu úlohu.

Uvedete-li ThreadedListener= NO, modul listener bez podprocesů (AMQCLMAA) spustí novou úlohu odpovídajícího modulu (AMQCRSTA) pro každý přichodící kanál TCP/IP. Nevýhodou této techniky je, že není tak rychlé spuštění nové úlohy AMQCRSTA, protože má spustit podproces v rámci úlohy RUNMQLSR, proto jsou časy připojení pro modul listener bez podprocesů pomalejší než u posluchače podprocesů s podporou podprocesů.

AdoptNewMCA= **NO** | SVR | SNDR | RCVR | CLUSRCVR | ALL | FASTPATH

Pokud příkaz IBM MQ obdrží požadavek na spuštění kanálu, ale zjistí, že pro stejný kanál existuje proces amqcst., musí být existující proces zastaven před tím, než může být nový spuštěn. Atribut AdoptNewMCA vám umožňuje kontrolovat ukončení existujícího procesu a spuštění nového typu pro uvedený typ kanálu.

Uvedete-li atribut AdoptNewMCA pro daný typ kanálu, ale nový kanál se nespustí, protože kanál je již spuštěn:

1. Nový kanál se pokusí o ukončení předchozí zprávy.
2. Pokud se předchozí server kanálu neukončí o čas, kdy vyprší interval čekání AdoptNewMCATimedout, proces (nebo podproces) pro předchozí kanál serveru je ukončen.
3. Pokud předchozí server kanálů nebyl ukončen po kroku 2 a poté, co vyprší interval čekání AdoptNewMCATimeout podruhé, produkt IBM MQ ukončí kanál s chybou CHANNEL IN USE .

Uvedete jednu nebo více hodnot oddělených čárkami nebo mezerami, z následujícího seznamu:

NO

Funkce AdoptNewMCA není povinná. Toto nastavení je výchozí.

SVR

Převzetí kanálů serveru

SNDR

Převzetí kanálů odesílatele

RCVR

převzetí přijímacích kanálů

CLUSRCVR

Převzetí přijímacích kanálů klastru

ALL

Převzetí všech typů kanálů, kromě kanálů FASTPATH

Rychlý

Převzetí kanálu v případě, že se jedná o kanál FASTPATH. K tomu dojde pouze v případě, že je zadán také vhodný typ kanálu, například AdoptNewMCA=RCVR, SVR, FASTPATH.

Pozor! Atribut MCA AdoptNewse může chovat nepředvídatelně s kanály FASTPATH kvůli vnitřnímu návrhu správce front. Dávejte si velkou opatrnost při povolování atributu AdoptNewMCA pro kanály FASTPATH.

AdoptNewMCATimeout= 60 | 1-3600

Doba (v sekundách), po kterou nový proces čeká na ukončení starého procesu. Uveďte hodnotu (v sekundách) v rozsahu 1-3600. Výchozí hodnota je 60.

AdoptNewMCACheck = QM | ADDRESS | NAME | ALL

Atribut AdoptNewMCACheck vám umožňuje uvést kontrolu typu, která se požaduje při povolení atributu AdoptNewMCA. Je důležité provést všechny tři následující kontroly, je-li to možné, abyste ochránili vaše kanály před vypnutím, nechtěně nebo neúmyslně nebo neúmyslně. Přinejmenším zkontrolujte, zda se názvy kanálů shodují.

Uveďte jednu nebo více hodnot oddělených čárkami nebo mezerami, z následujících možností:

QM

Proces modulu listener zkontroluje, zda se názvy správce front shodují.

ADDRESS

Proces modulu listener kontroluje komunikační adresu, například adresu TCP/IP.

NAME

Proces modulu listener zkontroluje, zda se shodují názvy kanálů.

ALL

Proces modulu listener vyhledá odpovídající názvy správců front, komunikační adresu a odpovídající názvy kanálů.

Výchozí hodnota je AdoptNewMCACheck=NAME, ADDRESS, QM.

Související pojmy

“Stavy kanálů” na stránce 154

Kanál může být v libovolném okamžiku v některém z mnoha stavů. Některé stavy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

**stanza QMErrorLog na systému IBM i**

Pomocí objektu stanza QMErrorLog v souboru qm.ini můžete upravit provoz a obsah protokolů chyb správce front.

ErrorLogVelikost = maxsize

Uvádí velikost protokolu chyb správce front, ve kterém je kopírován do zálohování. Hodnota maxsize musí být v rozsahu od 1048576 do 2147483648 bajtů. Není-li parametr ErrorLogSize zadán, bude použita výchozí hodnota 2097152 bajtů (2 MB).

ExcludeMessage= msgIds

Určuje zprávy, které nemají být zapsány do protokolu chyb správce front. msgIds obsahují čárkami oddělený seznam ID zpráv z následujících:

7163 - Zpráva o spuštění úlohy (pouze IBM i).

7234 - Počet načtených zpráv.

9001 - Program kanálu byl standardně ukončen.

9002 - Program kanálu byl spuštěn.

9202 - Vzdálený hostitel je nedostupný.
9208-Chyba při příjmu z hostitele
9209-Připojení bylo ukončeno.
9228-Nelze spustit odpovídací modul kanálu
9508-Nelze se připojit ke správci front
9524 - Vzdálený správce front je nedostupný.
9528 - Zavření kanálu vyžadované uživatelem.
9558-Vzdálený kanál není k dispozici
9776-Kanál byl blokován podle ID uživatele
9777-Kanál NOACCESS byl blokován kanálem.
9782-Spojení bylo blokováno adresou
9999 - Program kanálu byl ukončen nestandardně.

SuppressMessage= *msgIds*

Určuje zprávy, které budou zapsány do protokolu chyb správce front pouze jednou za určený časový interval. Časový interval je určen parametrem SuppressInterval . *msgIds* obsahují čárkami oddělený seznam ID zpráv z následujících:

7163 - Zpráva o spuštění úlohy (pouze IBM i).
7234 - Počet načtených zpráv.
9001 - Program kanálu byl standardně ukončen.
9002 - Program kanálu byl spuštěn.
9202 - Vzdálený hostitel je nedostupný.
9208-Chyba při příjmu z hostitele
9209-Připojení bylo ukončeno.
9228-Nelze spustit odpovídací modul kanálu
9508-Nelze se připojit ke správci front
9524 - Vzdálený správce front je nedostupný.
9528 - Zavření kanálu vyžadované uživatelem.
9558-Vzdálený kanál není k dispozici
9776-Kanál byl blokován podle ID uživatele
9777-Kanál NOACCESS byl blokován kanálem.
9782-Spojení bylo blokováno adresou
9999 - Program kanálu byl ukončen nestandardně.

Je-li v obou SuppressMessage a ExcludeMessage uvedeno stejné ID zprávy, tato zpráva je vyloučena.

SuppressInterval= *délka*

Určuje časový interval (v sekundách), ve kterém budou zprávy zadané v SuppressMessage zapsány do protokolu chyb správce front pouze jednou. *délka* musí být v rozsahu 1 až 86400 sekund. Není-li parametr SuppressInterval zadán, použije se výchozí hodnota 30 sekund.

Sekce TCP

Chcete-li zadat parametry konfigurace síťového protokolu, použijte tyto stránky vlastností správce front nebo oddíly v souboru `qm.ini`. Přepisují výchozí atributy pro kanály.

Poznámka: Je třeba zadat pouze atributy představující změny výchozích hodnot.

TCP

Je možné zadat následující atributy:

Port = 1414 | číslo_portu

Výchozí číslo portu pro relace TCP/IP v desítkové notaci. Výchozí číslo portu pro produkt IBM MQ 8.0 je 1414.

KeepAlive= NO |YES

Vypněte funkci KeepAlive zapnutou nebo vypnutou. KeepAlive=ANO způsobí, že TCP/IP pravidelně kontroluje, zda je druhý konec připojení stále dostupný. Není-li tomu tak, kanál je uzavřen.

ListenerBacklog= číslo

Při příjmu v protokolu TCP/IP je nastaven maximální počet neprovedených požadavků na připojení. To může být považováno za *nevyřízené požadavky* požadavků čekajících na portu TCP/IP pro modul listener, aby přijal požadavek. Výchozí hodnota nevyřízených požadavků listeneru pro IBM i je 255; maximum je 512. Pokud velikost nevyřízených požadavků dosáhne hodnoty 512, je připojení TCP/IP odmítnuto a kanál nelze spustit.

V případě kanálu MCA se výsledkem tohoto výsledku v kanálu stane stav ZOPAKOVAT a později se znovu pokusí o připojení.

V případě připojení klienta obdrží klient kód příčiny MQRQ_Q_MGR_NOT_AVAILABLE z MQCONN a měl by se k připojení znovu pokusit později.

Atribut ListenerBacklog umožňuje potlačit výchozí počet nevyřízených požadavků na modul listener protokolu TCP/IP.

Connect_Timeout = číslo | 0

Počet sekund před pokusem o připojení k vypršení časového limitu soketu. Výchozí hodnota nula určuje, že časový limit připojení neexistuje.

Následující skupinu vlastností lze použít k řízení velikosti vyrovnávacích pamětí používaných TCP/IP. Hodnoty jsou předávány přímo do vrstvy TCP/IP operačního systému. Při používání těchto vlastností je třeba věnovat velkou pozornost. Jsou-li hodnoty nastaveny nesprávně, může to nepříznivě ovlivnit výkon TCP/IP. Další informace o tom, jak to ovlivní výkon, najdete v dokumentaci TCP/IP pro vaše prostředí. Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, a to na rozdíl od velikosti vyrovnávací paměti, které jsou opraveny produktem IBM MQ.

SndBuffVelikost=číslo | 0

Velikost odesílací vyrovnávací paměti TCP/IP použité odesílajícím koncem kanálů v bajtech. Tato hodnota stanzy může být přepsána oddílem specifitěji pro daný typ kanálu, například RcvSndBuffSize.

RcvBuffVelikost=číslo | 0

Velikost vyrovnávací paměti pro příjem TCP/IP používaného přijímajícím koncem kanálů, v bajtech. Tato hodnota stanzy může být přepsána oddílem specifitěji pro typ kanálu, například RcvRcvBuffSize. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

RcvSndBuffSize= číslo | 0

Velikost vyrovnávací paměti pro odesílání protokolu TCP/IP v bajtech použitá odesílacím koncem přijímacího kanálu. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

RcvRcvBuffSize= číslo | 0

Velikost vyrovnávací paměti pro příjem TCP/IP používaného přijímajícím koncem kanálu příjemce, v bajtech. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

SvrSndBuffSize= číslo | 0

Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá na konci serveru pro kanál připojení serveru připojení klienta. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

SvrRcvBuffSize= číslo | 0

Velikost vyrovnávací paměti pro příjem protokolu TCP/IP v bajtech použitá na konci serveru kanálu připojení klienta pro připojení klienta k serveru. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

Příklad souborů IBM i mqs.ini a qm.ini

Příklad konfiguračního souboru IBM MQ

Následující příklad ukazuje soubor mqs.ini pro IBM i:

```
#####  
#* Module Name: mqs.ini *#  
#* Type : IBM MQ Configuration File *#  
#* Function : Define IBM MQ resources for the node *#  
#* *#  
#* Notes : *#  
#* 1) This is an example IBM MQ configuration file *#  
#* *#  
#####  
AllQueueManagers:  
#* The path to the qmgrs directory, within which queue manager data *#  
#* is stored *#  
#* *#  
DefaultPrefix=/QIBM/UserData/mqm  
  
QueueManager:  
Name=saturn.queue.manager  
Prefix=/QIBM/UserData/mqm  
Library=QMSATURN.Q  
Directory=saturn!queue!manager  
  
QueueManager:  
Name=pluto.queue.manager  
Prefix=/QIBM/UserData/mqm  
Library=QMPLUTO.QU  
Directory=pluto!queue!manager  
  
DefaultQueueManager:  
Name=saturn.queue.manager
```

Příklad konfiguračního souboru správce front

Následující příklad ukazuje, jak mohou být skupiny atributů uspořádány v konfiguračním souboru správce front produktu IBM i.

```
#####  
#* Module Name: qm.ini *#  
#* Type : IBM MQ queue manager configuration file *#  
#* Function : Define the configuration of a single queue manager *#  
#* *#  
#* Notes : *#  
#* 1) This file defines the configuration of the queue manager *#  
#* *#  
#####  
Log:  
LogPath=QMSATURN.Q  
LogReceiverSize=65536  
  
CHANNELS:  
MaxChannels = 20 ; Maximum number of channels allowed.  
; Default is 100.  
MaxActiveChannels = 10 ; Maximum number of channels allowed to be  
; active at any time. The default is the  
; value of MaxChannels.  
  
TCP: ; TCP/IP entries.  
KeepAlive = Yes ; Switch KeepAlive on.  
SvrSndBuffSize=20000 ; Size in bytes of the TCP/IP send buffer for each  
; channel instance. Default is 32768.  
SvrRcvBuffSize=20000 ; Size in bytes of the TCP/IP receive buffer for each  
; channel instance. Default is 32768.  
Connect_Timeout=10000 ; Number of seconds before an attempt to connect the  
; channel instance times out. Default is zero (no timeout).  
  
QMErrorLog:  
ErrorLogSize = 262144  
ExcludeMessage = 7234
```

```
SuppressMessage = 9001,9002,9202  
SuppressInterval = 30
```

Notes:

1. IBM MQ v uzlu používá výchozí umístění pro správce front a žurnály.
2. Správce front saturn.queue.manager je výchozím správcem front pro uzel. Adresář pro soubory přidružené k tomuto správci front byl automaticky transformován do platného názvu souboru pro systém souborů.
3. Protože konfigurační soubor produktu IBM MQ se používá k vyhledání dat přidružených ke správcům front, může neexistující nebo chybný konfigurační soubor způsobit selhání některých nebo všech příkazů IBM MQ . Aplikace se také nemohou připojit ke správci front, který není definován v konfiguračním souboru IBM MQ .

Atributy pro změnu konfiguračních informací IBM MQ

V systémech IBM MQ for Windows a v systémech IBM MQ for Linux (platformy x86 a x86-64) upravte konfigurační informace pomocí Průzkumníka IBM MQ . V jiných systémech upravte informace úpravou konfiguračního souboru mq.s.ini .

Prohlédněte si následující dílčí témata pro atributy pro specifické komponenty:

Související pojmy

[“Konfigurace” na stránce 5](#)

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

[“Změna konfiguračních informací IBM MQ a správce front” na stránce 81](#)

Změňte chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související odkazy

[“Změna konfiguračních informací správce front” na stránce 105](#)

Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro IBM MQ.

Související informace

[Naplánování](#)

[Správa serveru IBM MQ](#)

Všichni správci front

Použijte stránku vlastností General a Extended IBM MQ ze sekce MQ Explorer nebo AllQueueManagers v souboru mq.s.ini a zadejte následující informace o všech správcích front.

DefaultPrefix= *název_adresáře*

Tento atribut určuje cestu k adresáři qmgrs, v němž jsou uložena data správce front.

Pokud změníte výchozí předponu pro správce front, replikujte adresářovou strukturu, která byla vytvořena při instalaci.

Zejména je třeba vytvořit strukturu qmgrs. Zastavte IBM MQ před změnou výchozí předpony a restartujte IBM MQ až poté, co jste přesunuli struktury do nového umístění a změnili výchozí předponu.

Poznámka: Neodstraňujte adresář /var/mqm/errors v systémech SYSTÉM UNIX a Linux , ani adresář \errors v systémech Windows .

Jako alternativu ke změně výchozí předpony můžete použít proměnnou prostředí MQSPREFIX k potlačení DefaultPrefix pro příkaz crtmqm .

Vzhledem k omezením operačního systému zachovejte dodanou cestu dostatečně krátkou tak, aby součet délky cesty a libovolného názvu správce front byl maximálně 70 znaků dlouhý.

ConvEBCDICNewline= NL_TO_LF | TABLE | ISO

Kódové stránky EBCDIC obsahují znak nového řádku (NL), který není podporován kódovými stránkami ASCII (ačkoli některé varianty ISO obsahující ASCII obsahují ekvivalent). Atribut ConvEBCDICNewline použijte k uvedení, jak se má IBM MQ převést znak NL EBCDIC do formátu ASCII.

z/OS Atribut ConvEBCDICNewline není k dispozici v produktu z/OS. Chování v systému z/OS je ekvivalentní příkazu ConvEBCDICNewline=TABLE. Všimněte si, že výchozí nastavení na jiných platformách může být odlišné.

NL_TO_LF

Konvertuje znak NL (X'15 ') EBCDIC na znak LF (LF (X'0A')), pro všechny převody z formátu EBCDIC na ASCII.

Výchozí hodnota NL_TO_LF je výchozí.

TABULKA

Převedte znak NL kódové stránky EBCDIC podle převodních tabulek používaných na vaší platformě pro všechny převody z formátu EBCDIC na ASCII.

Vliv tohoto typu převodu se může lišit od platformy k platformě a z jazyka do jazyka; dokonce i na stejné platformě se může chování lišit, pokud použijete odlišné CCSID.

ISO

Převést:

- CCSID ISO pomocí metody TABLE
- Všechny ostatní CCSID používající metodu NL_TO_CF

Možné identifikátory CCSID ISO jsou zobrazeny v [Tabulka 12 na stránce 99](#).

CCSID	Kódová sada
819	ISO8859-1
912	ISO8859-2
915	ISO8859-5
1089	ISO8859-6
813	ISO8859-7
916	ISO8859-8
920	ISO8859-9
1051	roman8

Není-li ASCII CCSID podmnožinou ISO, ConvEBCDICNewline standardně zobrazuje NL_TO_LF.

V 8.0.0.12 V produktu IBM MQ 8.0.0, opravná sada Fix Pack 12 můžete místo atributu stanza **ConvEBCDICNewline** použít proměnnou prostředí **AMQ_CONVEBCDICNEWLINE**, například pro poskytnutí funkce **ConvEBCDICNewline** na straně klienta v situacích, kdy nelze použít soubor `mqc.ini`. Proměnná prostředí má stejné hodnoty (NL_TO_LF, TABLE, nebo ISO) jako atribut **ConvEBCDICNewline**. Atribut stanzy má přednost, je-li nastaven atribut i proměnná prostředí.

Předvolený správce fronty

Pomocí stránky vlastností produktu General IBM MQ v Průzkumníku IBM MQ nebo ze stanzy `DefaultQueueManager` v souboru `mqc.ini` určete výchozího správce front.

Název = *výchozí_správce_front*

Výchozí správce front zpracovává všechny příkazy, pro které není explicitně určen název správce front. Atribut `DefaultQueueManager` se automaticky aktualizuje, pokud vytvoříte nového výchozího správce front. Pokud jste neúmyslně vytvořili nového výchozího správce front a poté se chcete vrátit k původnímu správci front, změňte atribut `DefaultQueueManager` ručně.

Vlastnosti uživatelské procedury

Na stránce vlastností produktu `Extended IBM MQ` v Průzkumníku `IBM MQ` nebo v objektu stanza `ExitProperties` v souboru `mqs.ini` určete volby konfigurace používané uživatelskými programy správce front.

CLWLMode= **SAFE | FAST**

Ukončení pracovní zátěže klastru (CLWL) vám umožňuje určit, která fronta klastru v klastru má být otevřena v rámci odezvy na volání MQI (například `MQOPEN`, `MQPUT`). Uživatelská procedura CLWL se spustí buď v režimu **FAST**, nebo v režimu **SAFE**, v závislosti na hodnotě, kterou zadáte v atributu `CLWLMode`. Pokud vynecháte atribut `CLWLMode`, uživatelská procedura pracovní zátěže klastru se spustí v režimu **SAFE**.

SAFE

Spusťte uživatelskou proceduru CLWL v odděleném procesu od správce front. Toto nastavení je výchozí.

Pokud se vyskytne problém s uživatelskou procedurou CLWL, když je spuštěn v režimu **SAFE**, nastane následující situace:

- Proces serveru CLWL (`amqzlw0`) selže.
- Správce front restartuje proces serveru CLWL.
- Chyba je ohlášena v protokolu chyb. Pokud probíhá volání MQI, obdržíte oznámení ve formě návratového kódu.

Integrita správce front je zachována.

Poznámka: Spuštění uživatelské procedury CLWL v odděleném procesu může ovlivnit výkon.

FAST

Spusťte uživatelskou proceduru klastru vloženou do procesu správce front.

Zadáním této volby zvýšíte výkon tím, že se vyhnete nákladům na přepínání procesu, které jsou přidruženy ke spuštění v režimu **SAFE**, ale provádí se tak na úkor integrity správce front. Ukončení CLWL byste měli spustit pouze v režimu **FAST**, jste-li přesvědčeni, že při ukončení CLWL nejsou žádné problémy s **žádným** problémem, a vy jste obzvláště znepokojeni výkonem.

Pokud se vyskytne problém, když je uživatelská procedura CLWL spuštěna v režimu **FAST**, správce front selže a vy spustíte riziko, že integrita správce front bude ohrožena.

Předvolby protokolu pro IBM MQ

Na stránce vlastností produktu `Default log settings IBM MQ` v Průzkumníku `IBM MQ` nebo v objektu stanza `LogDefaults` v souboru `mqs.ini` zadejte informace o předvolbách protokolu pro všechny správce front.

Pokud objekt stanza neexistuje, použije se výchozí nastavení MQ. Atributy protokolu se používají jako výchozí hodnoty při vytváření správce front, ale mohou být přepsány, pokud zadáte atributy protokolu v příkazu `crtmqm`. Podrobnosti o tomto příkazu viz [crtmqm](#).

Jakmile je správce front vytvořen, budou atributy protokolu tohoto správce front převzaty z nastavení popsaných v tématu [“Protokoly správce front”](#) na stránce 109.

Výchozí předpona (uvedená v [“Všichni správci front”](#) na stránce 98) a cesta k protokolu určená pro konkrétního správce front (uvedený v souboru [“Protokoly správce front”](#) na stránce 109) povolí správci front a jeho protokolu být na různých fyzických jednotkách. Toto je doporučená metoda, ačkoli při výchozím nastavení jsou na stejné jednotce.

Informace o výpočtu velikosti protokolu viz [“Výpočet velikosti protokolu”](#) na stránce 463.

Poznámka: Limity uvedené v následujícím seznamu parametrů jsou limity nastavené parametrem IBM MQ. Limity operačního systému mohou snížit maximální možnou velikost protokolu.

LogPrimarySoubory = 3 | 2-254 (Windows) | 2-510 (SYSTÉM UNIX a Linux systémy)

Soubory protokolu přidělené při vytvoření správce front.

Minimální počet primárních souborů protokolu, které můžete mít, je 2 a maximum je 254 na Windows, nebo 510 na systémech SYSTÉM UNIX a Linux . Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windows nebo 511 na systémech SYSTÉM UNIX a Linux a nesmí být menší než 3.

Hodnota je ověřována při vytváření nebo spouštění správce front. Po vytvoření správce front jej můžete změnit. Změna hodnoty však není účinná, dokud se správce front nerestartuje a účinek nemusí být okamžitý.

LogSecondarySoubory = 2 | 1-253 (Windows) | 1-509 (SYSTÉM UNIX a Linux systémy)

Soubory protokolu přidělené při vyčerpání primárních souborů.

Minimální počet sekundárních souborů protokolu je 1 a maximum je 253 na Windows, nebo 509 na systémech SYSTÉM UNIX a Linux . Výchozí hodnota je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windows nebo 511 na systémech SYSTÉM UNIX a Linux a nesmí být menší než 3.

Hodnota je přezkoumána, když je spuštěn správce front. Tuto hodnotu můžete změnit, ale změny se neprojeví, dokud nerestartujete správce front, a dokonce i tento efekt nemusí být okamžitý.

LogFilePages = číslo

Data protokolu jsou uchovávány v řadě souborů s názvem souborů protokolu. Velikost souboru protokolu je určena v jednotkách 4kB stránek.

Výchozí počet stránek souboru protokolu je 4096, což dává velikost souboru protokolu 16 MB.

V systémech SYSTÉM UNIX a Linux je minimální počet stránek souboru protokolu 64 a v systému Windows je minimální počet stránek souboru protokolu 32; v obou případech je maximální počet 65 535.

Poznámka: Velikost souborů žurnálu uvedených během vytváření správce front nelze změnit pro správce front.

LogType= CIRCULAR | LINEAR

Typ protokolu, který má být použit. Výchozí hodnota je CIRCULAR.

CIRCULAR

Spustíte zotavení restartováním pomocí protokolu k odvolání transakcí, které probíhaly, když se systém zastavil.

Podrobnější vysvětlení kruhového protokolování naleznete v příručce [“Typy protokolování”](#) na stránce 458 .

Lineární

Pro restartování obnovy a média nebo dopředné zotavení (vytváření ztracených nebo poškozených dat opětovným přehráváním obsahu protokolu).

Bližší vysvětlení lineárního protokolování najdete v části [“Typy protokolování”](#) na stránce 458 .

Chcete-li změnit výchozí nastavení, můžete buď upravit atribut LogType , nebo zadat lineární protokolování pomocí příkazu `crtmqm` . Metodu protokolování nelze změnit poté, co byl vytvořen správce front.

LogBufferStránky = 0 | 0-4096

Množství paměti přidělené pro zápis do vyrovnávací paměti a určuje velikost vyrovnávacích pamětí v jednotkách 4kB stránek.

Minimální počet stránek vyrovnávací paměti je 18 a maximum je 4096. Větší vyrovnávací paměti přispívají k vyšší propustnosti, zvláště velkých zpráv.

Jestliže uvedete 0 (předvolba), správce front vybere velikost. V IBM WebSphere MQ 7.1 je to 512 (2048 kB).

Zadáte-li číslo v rozsahu od 1 do 17, správce front bude standardně zobrazovat 18 (72 kB). Určíte-li číslo v rozsahu 18 až 4096, správce front použije zadané číslo k nastavení přidělené paměti.

LogDefaultPath = *název_adresáře*

Adresář, ve kterém jsou umístěny soubory žurnálu pro správce front. Adresář je umístěn v lokálním zařízení, do kterého může správce front zapisovat, a pokud možno na jiné jednotce z front zpráv. Zadání jiné jednotky poskytuje ochranu v případě selhání systému.

Výchozí nastavení je:

- <DefaultPrefix>\log pro IBM MQ for Windows , kde <DefaultPrefix> je hodnota zadaná na atributu DefaultPrefix na stránce vlastností All Queue Managers IBM MQ . Tato hodnota je nastavena při instalaci.
- /var/mqm/log pro systémy IBM MQ for UNIX a Linux

Jinou možností je zadat název adresáře v příkazu crtmqm pomocí příznaku -ld. Při vytvoření správce front je v adresáři správce front vytvořen také adresář a tento adresář se používá k uchování souborů protokolu. Název tohoto adresáře je založen na názvu správce front. Tím je zajištěno, že cesta k souboru protokolu je jedinečná a že je v souladu s omezeními délkou názvu adresáře.

Pokud u příkazu crtmqm nezadáte hodnotu -ld, bude použita hodnota atributu LogDefaultPath v souboru mqsc.ini .

Název správce front je připojen k názvu adresáře, aby bylo zajištěno, že více správců front používá různé adresáře protokolů.

Při vytvoření správce front je v attributech protokolu v informacích o konfiguraci vytvořena hodnota LogPath , která obsahuje úplný název adresáře pro protokol správce front. Tato hodnota se používá k vyhledání protokolu při spuštění nebo odstranění správce front.

LogWriteIntegrity = SingleWrite|DoubleWrite| TripleWrite

Metoda, kterou modul protokolování používá ke spolehlivému zápisu záznamů protokolu.

TripleWrite

Jedná se o výchozí metodu.

Všimněte si, že lze vybrat volbu **DoubleWrite**. Když tak ale uděláte, systém to interpretuje jako volbu **TripleWrite**.

SingleWrite

Měli byste použít **SingleWrite**, pouze pokud souborový systém a zařízení, které jsou hostiteli protokolu pro zotavení produktu IBM MQ , explicitně zaručuje atomičnost 4KB zápisů.

Když se tedy zápis 4kB stránky nezdaří z nějakého důvodu, jsou možné jen dva stavy: před obrazem nebo po obrazu. Žádný mezistav by neměl být možný.

Poznámka: Je-li v trvalé pracovní zátěži dostatečná souběžnost, existuje minimální potenciální přínos při nastavení jiných položek než výchozí hodnoty **TripleWrite**.

rozhraní Advanced Configuration and Power Interface (ACPI)

Použijte stránku vlastností produktu ACPI IBM MQ z Průzkumníka IBM MQ , abyste určili, jak se má IBM MQ chovat, když systém obdrží požadavek na pozastavení.

Produkt Windows podporuje standard ACPI (Advanced Configuration and Power Interface). To umožňuje uživatelům produktu Windows s povoleným ACPI hardware zastavit a restartovat kanály, když systém vstoupí do režimu pozastavení a obnoví se z režimu pozastavení.

Všimněte si, že nastavení uvedená na stránce vlastností produktu ACPI IBM MQ se použijí pouze tehdy, je-li monitor výstrah spuštěn. Pokud je monitor výstrah spuštěn, je na hlavním panelu zobrazena ikona Monitor výstrah.

DoDialog= Y | N

Zobrazí dialogové okno v době požadavku na pozastavení.

DenySuspend= Y | N

Odepírá požadavek na pozastavení. Používá se, pokud DoDialog= N, nebo pokud DoDialog= Y a dialogové okno nelze zobrazit, například, protože je víko vašeho notebooku zavřeno.

CheckChannelsRunning=Y | N

Zkontroluje, zda jsou spuštěny nějaké kanály. Výsledek může určit výsledek ostatních nastavení.

Následující tabulka ukazuje vliv každé kombinace těchto parametrů:

DoDialog	DenySuspend	Spuštění CheckChannels	Akce
N	N	N	Přijměte požadavek na pozastavení.
N	N	Y	Přijměte požadavek na pozastavení.
N	Y	N	Zamítnout požadavek na pozastavení.
N	Y	Y	Jsou-li některé kanály spuštěny, pozastavte požadavek na pozastavení; pokud žádost nepřijmete.
Y	N	N	Zobrazit dialogové okno (viz Poznámka ; přijmout požadavek na pozastavení). Toto nastavení je výchozí.
Y	N	Y	Pokud nejsou spuštěny žádné kanály, přijměte požadavek na pozastavení; pokud se zobrazí, zobrazí se toto dialogové okno (viz Poznámka). akceptujte požadavek).
Y	Y	N	Zobrazit dialogové okno (Poznámka ; odepřít požadavek na pozastavení).
Y	Y	Y	Pokud nejsou spuštěny žádné kanály, přijměte požadavek na pozastavení; pokud se zobrazí, zobrazí se dialogové okno (Poznámka ; zamítlí požadavek).

Poznámka: V případě, že akce má zobrazit dialogové okno, nelze-li dialogové okno zobrazit (například protože je zavřen kryt notebooku), použije se volba DenySuspend k určení, zda je požadavek na pozastavení přijat nebo odepřen.

Uživatelské procedury rozhraní API

Chcete-li změnit položky pro ukončení rozhraní API, použijte příkaz MQ Explorer nebo `amqmdain` .

Pomocí stránky vlastností produktu Exits IBM MQ ze souboru MQ Explorernebo stanzy `ApiExitTemplate` a `ApiExitCommon` v souboru `mqs.ini` můžete identifikovat rutiny ukončení rozhraní API pro všechny správce front. Na systémech Windows můžete také použít příkaz `amqmdain` ke změně položek pro ukončení rozhraní API. (Chcete-li identifikovat rutiny ukončení rozhraní API pro jednotlivé správce front, použijte stanzy `ApiExitLocal` , jak je popsáno v části [“Uživatelské procedury rozhraní API”](#) na stránce 119.)

Úplný popis atributů těchto stanz naleznete v tématu [Konfigurace uživatelských procedur rozhraní API](#).

Správci front

Pro každého správce front je zde jedna stanza `QueueManager`. Použijte sekci k určení umístění adresáře správce front.

Na systémech Windows, SYSTÉM UNIX a Linux existuje jeden objekt stanza `QueueManager` pro každého správce front. Tyto atributy určují název správce front a název adresáře, který obsahuje soubory přidružené k tomuto správci front. Název adresáře je založen na názvu správce front, ale v případě, že název správce front není platným názvem souboru, je transformován. Další informace o transformaci názvu viz téma [Základní informace o názvech souborů produktu IBM MQ](#).

Název = `queue_manager_name`

Název správce front.

Předpona = `předpona`

Kde jsou uloženy soubory správce front. Při výchozím nastavení je tato hodnota stejná jako hodnota zadaná v atributu `DefaultPrefix` v informacích o všech správcích front.

Adresář = `název`

Název podadresáře pod adresářem `<prefix>\QMGRS`, kde jsou uloženy soubory správce front. Tento název je založen na názvu správce front, lze jej však transformovat, pokud existuje duplicitní název, nebo pokud název správce front není platným názvem souboru.

DataPath= `cesta`

Explicitní cesta k datům, která byla poskytnuta při vytvoření správce front, potlačují předponu a adresář jako cestu k datům správce front.

InstallationName= `název`

Název instalace produktu IBM MQ přidružené k tomuto správci front. Příkazy z této instalace musí být použity při interakci s tímto správcem front. Není-li přítomna hodnota `InstallationName`, je správce front přidružen k instalaci produktu IBM MQ starší než Verze 7.1.

Související pojmy

“Přidružení správce front k instalaci” na stránce 362

Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz `crtmqm`. V systému SYSTÉM UNIX, Linuxu Oknamůžete změnit instalaci přidruženou ke správci front pomocí příkazu `setmqm`.

Zabezpečení

Použijte sekci `Security` v souboru `qm.ini`, abyste uvedli volby pro OAM (Object Authority Manager).

ClusterQueueAccessControl= `RQMName | Xmitq`

Nastavte tento atribut, chcete-li zkontrolovat řízení přístupu k frontám klastru nebo plně kvalifikovaným frontám hostovaným na správcích front klastru.

RQMNAME

Profily zkontrolované pro řízení přístupu vzdáleně hostovaných front jsou pojmenované fronty nebo pojmenované profily správce front.

XMITQ

Profily zkontrolované pro řízení přístupu vzdáleně hostovaných front jsou rozlišeny jako `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Výchozí hodnota je `Xmitq`.

GroupModel= `GlobalGroups`

Tento atribut určuje, zda produkt OAM kontroluje globální skupiny při určování členství ve skupině pro uživatele v systému Windows.

Předvolba je nekontrolovat globální skupiny.

GlobalGroups

OAM kontroluje globální skupiny.

Pomocí sady `GlobalGroups` přijímají autorizační příkazy, `setmqaut`, `dspmqa` a `dmpmqaut` globální názvy skupin, viz parametr [setmqaut -g](#).

Poznámka: Nastavení produktu `ClusterQueueAccessControl=RQMName` a vlastní implementace autorizační služby na méně než `MQZAS_VERSION_6` výsledků ve správci front se nespouští. V této instanci buď nastavte `ClusterQueueAccessControl=Xmitq`, nebo upgradujte vlastní autorizační službu na `MQZAS_VERSION_6` nebo vyšší.

Změna konfiguračních informací správce front

Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro IBM MQ.

V systémech SYSTÉM UNIX a Linux upravíte konfigurační informace správce front úpravou konfiguračního souboru produktu `qm.ini`. Definujete-li sekci v produktu `qm.ini`, nemusíte každou položku spouštět na novém řádku. K označení komentáře můžete použít buď středník (;), nebo hašovací znak (#).

V systémech Windows a Linux x86-64 můžete upravit některé informace o konfiguraci pomocí produktu MQ Explorer. Avšak protože existují významné důsledky pro změnu instalovatelných služeb a jejich komponent, instalovatelné služby jsou jen pro čtení v MQ Explorer. Proto musíte provést jakékoli změny instalovatelných služeb pomocí produktu **regedit** v systému Windowsa úpravou souboru `qm.ini` v systému SYSTÉM UNIX a Linux.

Další informace o změně informací o konfiguraci správce front naleznete v následujících dílčích tématech:

Související pojmy

[“Konfigurace” na stránce 5](#)

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

[“Změna konfiguračních informací IBM MQ a správce front” na stránce 81](#)

Změňte chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související odkazy

[“Atributy pro změnu konfiguračních informací IBM MQ” na stránce 98](#)

V systémech IBM MQ for Windows a v systémech IBM MQ for Linux (platformy x86 a x86-64) upravte konfigurační informace pomocí Průzkumníka IBM MQ. V jiných systémech upravte informace úpravou konfiguračního souboru `mqs.ini`.

Související informace

[Naplánování](#)

[Správa serveru IBM MQ](#)

Režim přístupu

Access Mode platí pouze pro servery Windows. Objekt stanza `AccessMode` je nastaven volbou `-a [r]` u příkazu `crtmqm`. Neměňte sekci `AccessMode` poté, co byl vytvořen správce front.

Použit skupinu přístupů (`-a [r]`) pomocí volby příkazu `crtmqm` určete skupinu zabezpečení produktu Windows, jejíž členové budou udělen úplný přístup ke všem datovým souborům správce front. Skupina může být buď lokální, nebo globální skupina, v závislosti na použité syntaxi. Platná syntaxe názvu skupiny je následující:

LocalGroup

Název domény\GlobalGroup

GlobalGroup @ Název domény

Před spuštěním příkazu `crtmqm` s volbou `-a [r]` je třeba definovat další skupinu přístupů.

Uvedete-li skupinu pomocí `-a r` místo `-a`, lokální skupina `mqm` nebude mít udělen přístup k datovým souborům správce front. Tuto volbu použijte, pokud systém souborů, který je hostitelem datových souborů správce front, nepodporuje položky řízení přístupu pro lokálně definované skupiny.

Skupina je obvykle skupina globálního zabezpečení, která se používá k zajištění správců front pro více instancí s přístupem k datům správce sdílených front a složce protokolů. Pomocí další skupiny

zabezpečeného přístupu můžete nastavit oprávnění ke čtení a zápisu k této složce, nebo sdílet data a soubory protokolu příslušného správce front.

Další skupina zabezpečení přístupu je alternativou k použití lokální skupiny s názvem mqm, která nastavuje oprávnění ke složce obsahující data a protokoly správce front. Na rozdíl od lokální skupiny mqm můžete vytvořit další skupinu zabezpečení přístupu ve formě lokální nebo globální skupiny. Chcete-li nastavovat oprávnění ke sdíleným složkám obsahujícím data a soubory protokolu používané správci front pro více instancí, musí se jednat o globální skupinu.

Operační systém Windows kontroluje oprávnění přístupu pro čtení a zápis do dat a souborů protokolu správce front. Kontroluje oprávnění ID uživatele, který spustil procesy správce front. Kontrolované ID uživatele závisí na tom, zda jste spustili správce front jako službu, nebo jste ho spustili interaktivně. Pokud jste spustili správce front jako službu, bude ID uživatele kontrolované systémem Windows ID uživatele, kterého jste nakonfigurovali v průvodci **Příprava produktu IBM MQ**. Pokud jste spustili správce front interaktivně, bude ID uživatele kontrolované systémem Windows ID uživatele, který spustil příkaz **strmqm**.

ID uživatele musí být členem lokální skupiny mqm, aby mohlo spustit správce front. Pokud je ID uživatele členem další skupiny zabezpečení přístupu, může správce front číst a zapisovat soubory s příslušnými oprávněními pomocí této skupiny.

Omezení: Pouze v operačním systému Windows můžete zadat další skupinu zabezpečení přístupu. Pokud zadáte další skupinu zabezpečení přístupu na jiném operačním systému, vrátí příkaz **crtmqm** chybu.

Související pojmy

[“Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows” na stránce 434](#)

[“Zabezpečte data správce sdílených front a soubory protokolu a soubory v systému Windows” na stránce 431](#)

Související úlohy

[“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény” na stránce 406](#)

Související informace

[crtmqm](#)

Instalovatelné služby

Instalovatelné služby můžete změnit na Windows pomocí **regedita** na SYSTÉM UNIX a Linux pomocí stanzy `Service` v souboru `qm.ini`.

Poznámka: Existují významné důsledky pro změnu instalovatelných služeb a jejich komponent. Z tohoto důvodu jsou instalovatelné služby určené pouze pro čtení v produktu MQ Explorer.

Chcete-li změnit instalovatelné služby na systémech Windows, použijte **regedit** nebo na systémech SYSTÉM UNIX a Linux, použijte stanzy `Service` v souboru `qm.ini`. Pro každou komponentu v rámci služby musíte zadat také název a cestu k modulu, který obsahuje kód dané komponenty. V systému SYSTÉM UNIX a Linux použijte pro tento objekt stanzy `ServiceComponent`.

Název = AuthorizationService |NameService

Název požadované služby.

AuthorizationService

Pro produkt IBM MQ je komponenta `AuthorizationService` známá jako správce oprávnění k objektu nebo OAM. Stanza `AuthorizationService` a přidružená stanzy `ServiceComponent` jsou automaticky přidány, když se vytvoří správce front. Přidejte další sekce `ServiceComponent` ručně.

NameService

Ve výchozím nastavení není poskytována žádná služba názvů. Požadujete-li službu názvů, musíte přidat sekci `NameService` ručně.

EntryPoints= počet-záznamů

Počet vstupních bodů definovaných pro službu.

To zahrnuje vstupní body inicializace a ukončení.

Windows SecurityPolicy= Default |NTSIDsRequired

V systémech Windows se atribut SecurityPolicy použije pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut SecurityPolicy vám umožňuje uvést zásady zabezpečení pro každého správce front.

Možné hodnoty jsou:

Default

Použijte výchozí zásady zabezpečení, které se mají použít. Pokud identifikátor zabezpečení produktu Windows (NT SID) není předán OAM pro konkrétní ID uživatele, provede se pokus o získání příslušného SID prohledáváním příslušných databází zabezpečení.

NTSIDsRequired

Při provádění kontrol zabezpečení předejte SID systému NT pro OAM.

Další informace viz [ID zabezpečení produktu Windows \(SID\)](#) .

Viz též [Configuring authorization service stanza: Windows systems](#).

Linux UNIX SecurityPolicy= uživatel|skupina | default

Na systémech SYSTÉM UNIX a Linux tato hodnota určuje, zda správce front používá autorizaci založenou na uživateli nebo na základě skupin. Hodnoty nejsou citlivé na velikost písmen.

Pokud tento atribut nezahrnete, použije se předvo1ba , která používá autorizaci založenou na skupině. Aby se změny projevily, restartujte správce front. Viz též [Configuring authorization service stanza: SYSTÉM UNIX a Linux systems](#).

SharedBindingsUserId= typ-uživatele

Atribut SharedBindingsUserId se použije pouze v případě, že uvedená služba je výchozí autorizační službou, to znamená OAM. Atribut SharedBindingsUserId se používá pouze se vztahem ke sdílenému vázání. Tato hodnota vám umožňuje uvést, zda je pole *UserIdentifier* ve struktuře *IdentityContext* z funkce MQZ_AUTHENTICATE_USER, je efektivním ID uživatele nebo skutečným ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu [MQZ_AUTHENTICATE_USER-Authenticate user](#).

Možné hodnoty jsou:

Default

Hodnota pole *UserIdentifier* je nastavena jako skutečné ID uživatele.

Fyzické

Hodnota pole *UserIdentifier* je nastavena jako skutečné ID uživatele.

Efektivní

Hodnota pole *UserIdentifier* je nastavena jako efektivní ID uživatele.

FastpathBindingsUserId= typ-uživatele

Atribut FastpathBindingsUserId se použije pouze v případě, že uvedená služba je výchozí autorizační službou, to znamená OAM. Atribut FastpathBindingsUserId se používá pouze s vazbou na vazby zkrácené cesty. Tato hodnota vám umožňuje uvést, zda je pole *UserIdentifier* ve struktuře *IdentityContext* z funkce MQZ_AUTHENTICATE_USER, je efektivním ID uživatele nebo skutečným ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu [MQZ_AUTHENTICATE_USER-Authenticate user](#).

Možné hodnoty jsou:

Default

Hodnota pole *UserIdentifier* je nastavena jako skutečné ID uživatele.

Fyzické

Hodnota pole *UserIdentifier* je nastavena jako skutečné ID uživatele.

Efektivní

Hodnota pole *UserIdentifier* je nastavena jako efektivní ID uživatele.

IsolatedBindingsUserId= typ-uživatele

Atribut **IsolatedBindingsUserId** se použije pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **IsolatedBindingsUserId** se používá pouze ve vztahu k izolovaným vazbám. Tato hodnota vám umožňuje uvést, zda je pole *UserIdentifier* ve struktuře *IdentityContext* z funkce MQZ_AUTHENTICATE_USER, je efektivním ID uživatele nebo skutečným ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu [MQZ_AUTHENTICATE_USER-Authenticate user](#).

Možné hodnoty jsou:

Default

Hodnota pole *UserIdentifier* je nastavena jako efektivní ID uživatele.

Fyzické

Hodnota pole *UserIdentifier* je nastavena jako skutečné ID uživatele.

Efektivní

Hodnota pole *UserIdentifier* je nastavena jako efektivní ID uživatele.

Další informace o instalovatelných službách a komponentách najdete v tématu [Instalovatelné služby a komponenty pro produkty UNIX, Linux a Windows](#).

Další informace o službách zabezpečení obecně najdete v tématu [Nastavení zabezpečení v systémech SYSTÉM UNIX a Linux](#).

Související informace

[Referenční informace o instalovatelných službách](#)

Servisní komponenty

Když přidáváte novou instalovatelnou službu, musíte uvést informace o komponentě služby. V systémech Windows použijte `regedit` a v systémech SYSTÉM UNIX a Linux použijte sekci `ServiceComponent` v souboru `qm.ini`. Sekce autorizační služby je standardně přítomná a přidružená komponenta, OAM, je aktivní.

Specifikujte komponenty služby takto:

Služba = název_služby

Název požadované služby. Musí odpovídat hodnotě zadané v atributu `Name` v informacích o konfiguraci služby.

Název = název_komponenty

Popisný název komponenty služby. Musí být jedinečný a obsahovat pouze znaky, které jsou platné pro názvy objektů produktu IBM MQ (například názvy front). Tento název se vyskytuje ve zprávách operátora generovaných službou. Doporučujeme, aby tento název začal ochrannou známkou společnosti nebo obdobným rozlišovacím řetězcem.

Modul = název_modulu

Název modulu, který má obsahovat kód pro tuto komponentu. Musí se jednat o úplný název cesty.

ComponentDataVelikost = velikost

Velikost (v bajtech) oblasti dat komponenty předaného komponentě při každém volání. Uvedte nulu, pokud nejsou požadována žádná data komponenty.

Další informace o instalovatelných službách a komponentách najdete v tématu [Instalovatelné služby a komponenty pro produkty UNIX, Linux a Windows](#).

Protokoly správce front

Použijte stránku vlastností správce front produktu Log z Průzkumníka IBM MQ nebo sekci Log v souboru qm.ini , abyste určili informace o protokolování správce front.

Ve výchozím nastavení jsou tato nastavení zděděna z nastavení určených pro výchozí nastavení protokolu správce front (popsáno v tématu [“Předvolby protokolu pro IBM MQ”](#) na stránce 100). Změňte tato nastavení pouze v případě, že chcete tohoto správce front nakonfigurovat jiným způsobem.

Informace o výpočtu velikosti protokolu viz [“Výpočet velikosti protokolu”](#) na stránce 463.

Poznámka: Limity uvedené v následujícím seznamu parametrů jsou nastaveny parametrem IBM MQ. Limity operačního systému mohou snížit maximální možnou velikost protokolu.

LogPrimarySoubory = 3 | 2-254 (Windows) | 2-510 (SYSTÉM UNIX a Linux systémy)

Soubory protokolu přidělené při vytvoření správce front.

Minimální počet primárních souborů protokolu, které můžete mít, je 2 a maximum je 254 na Windows, nebo 510 na systémech SYSTÉM UNIX a Linux . Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windows nebo 511 na systémech SYSTÉM UNIX a Linux a nesmí být menší než 3.

Hodnota je ověřována při vytváření nebo spouštění správce front. Po vytvoření správce front jej můžete změnit. Změna hodnoty však není účinná, dokud se správce front nerestartuje a účinek nemusí být okamžitý.

LogSecondarySoubory = 2 | 1-253 (Windows) | 1-509 (SYSTÉM UNIX a Linux systémy)

Soubory protokolu přidělené při vyčerpání primárních souborů.

Minimální počet sekundárních souborů protokolu je 1 a maximum je 253 na Windows, nebo 509 na systémech SYSTÉM UNIX a Linux . Výchozí hodnota je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windows nebo 511 na systémech SYSTÉM UNIX a Linux a nesmí být menší než 3.

Hodnota je přezkoumána, když je spuštěn správce front. Tuto hodnotu můžete změnit, ale změny se neprojeví, dokud nerestartujete správce front, a dokonce i tento efekt nemusí být okamžitý.

LogFilePages = číslo

Data protokolu jsou uchovávány v řadě souborů s názvem souborů protokolu. Velikost souboru protokolu je určena v jednotkách 4kB stránek.

Výchozí počet stránek souboru protokolu je 4096, což dává velikost souboru protokolu 16 MB.

V systémech SYSTÉM UNIX a Linux je minimální počet stránek souboru protokolu 64 a v systému Windows je minimální počet stránek souboru protokolu 32; v obou případech je maximální počet 65 535.

Poznámka: Velikost souborů žurnálu uvedených během vytváření správce front nelze změnit pro správce front.

LogType= CIRCULAR | LINEAR

Typ protokolování, který má používat správce front. Typ protokolování, který má být použit po vytvoření správce front, nelze změnit. Informace o vytvoření správce front s typem protokolování, které vyžadujete, naleznete v popisu atributu LogType v příručce [“Předvolby protokolu pro IBM MQ”](#) na stránce 100 .

CIRCULAR

Spusťte zotavení restartováním pomocí protokolu k odvolání transakcí, které probíhaly, když se systém zastavil.

Podrobnější vysvětlení kruhového protokolování naleznete v příručce [“Typy protokolování”](#) na stránce 458 .

Lineární

Pro restartování obnovy a média nebo dopředné zotavení (vytváření ztracených nebo poškozených dat opětovným přehráváním obsahu protokolu).

Bližnější vysvětlení lineárního protokolování najdete v části [“Typy protokolování”](#) na stránce 458 .

LogBufferStránky = 0 | 0-4096

Množství paměti přidělené pro zápis do vyrovnávací paměti a určuje velikost vyrovnávacích pamětí v jednotkách 4kB stránek.

Minimální počet stránek vyrovnávací paměti je 18 a maximum je 4096. Větší vyrovnávací paměti přispívají k vyšší propustnosti, zvláště velkých zpráv.

Jestliže uvedete 0 (předvolba), správce front vybere velikost. V IBM WebSphere MQ 7.1 je to 512 (2048 kB).

Zadáte-li číslo v rozsahu od 1 do 17, správce front bude standardně zobrazovat 18 (72 kB). Zadáte-li číslo v rozsahu od 18 do 4096, správce front použije zadané číslo k nastavení přidělené paměti.

Hodnota je přezkoumána, když je spuštěn správce front. Hodnota může být zvýšena nebo snížena v rámci uvedených limitů. Změna hodnoty však nebude efektivní až do příštího spuštění správce front.

LogPath= název_adresáře

Adresář, ve kterém jsou umístěny soubory žurnálu pro správce front. Tato hodnota musí existovat na lokálním zařízení, do kterého může správce front zapisovat a, pokud možno, na jiném disku z front zpráv. Zadání jiné jednotky poskytuje ochranu v případě selhání systému.

Výchozí nastavení je:

- C:\ProgramData\IBM\MQ\log v příručce IBM MQ for Windows.
- /var/mqm/log v systémech IBM MQ for UNIX a Linux .

Pomocí příznaku -ld lze zadat název adresáře v příkazu crtmqm . Při vytvoření správce front je v adresáři správce front vytvořen také adresář a tento adresář se používá k uchování souborů protokolu. Název tohoto adresáře je založen na názvu správce front. Tím je zajištěno, že cesta k souboru protokolu je jedinečná a že je v souladu s omezeními délkou názvu adresáře.

Pokud u příkazu crtmqm nezadáte parametr -ld, bude použita hodnota atributu LogDefaultPath .

V systémech IBM MQ for UNIX a Linux musí mít uživatel ID mqm a skupina mqm úplná oprávnění k souborům protokolu. Pokud změníte umístění těchto souborů, musíte tyto oprávnění poskytnout sami sobě. To není povinné, pokud jsou soubory protokolu ve výchozích umístěních dodaných s produktem.

LogWriteIntegrita =SingleWrite|DoubleWrite| TripleWrite

Metoda, kterou modul protokolování používá ke spolehlivému zápisu záznamů protokolu.

TripleWrite

Jedná se o výchozí metodu.

Všimněte si, že lze vybrat volbu **DoubleWrite**. Když tak ale uděláte, systém to interpretuje jako volbu **TripleWrite**.

SingleWrite

Měli byste použít **SingleWrite**, pouze pokud souborový systém a zařízení, které jsou hostiteli protokolu pro zotavení produktu IBM MQ , explicitně zaručuje atomičnost 4KB zápisů.

Když se tedy zápis 4kB stránky nezdaří z nějakého důvodu, jsou možné jen dva stavy: před obrazem nebo po obrazu. Žádný mezistav by neměl být možný.

Poznámka: Je-li v trvalé pracovní zátěži dostatečná souběžnost, existuje minimální potenciální přínos při nastavení jiných položek než výchozí hodnoty **TripleWrite**.

Omezený režim

Tato volba platí pouze pro systémy SYSTÉM UNIX a Linux . Stanza `RestrictedMode` je nastavena pomocí volby `-g` v příkazu `crtmqm` . Neměňte tuto stanci poté, co byl vytvořen správce front. Nepoužijete-li volbu `-g`, nebude objekt stanza vytvořen v souboru `qm.ini` .

Existují některé adresáře, v rámci kterých aplikace produktu IBM MQ vytvářejí soubory, zatímco jsou připojeny ke správci front v datovém adresáři správce front. Aby aplikace mohly vytvářet soubory v těchto adresářích, mají udělen přístup pro zápis do světa:

- `/var/mqm/sockets/QMgrName/@ipcc/ssem/hostname/`
- `/var/mqm/sockets/QMgrName/@app/ssem/hostname/`
- `/var/mqm/sockets/QMgrName/zsocketapp/hostname/`

kde `<QMGRNAME>` je název správce front a `<hostname>` je název hostitele.

Na některých systémech je nepřijatelné udělit všem uživatelům přístup pro zápis do těchto adresářů. Například ti, kteří nepotřebují přístup ke správci front. Omezený režim upravuje oprávnění k adresářům, které ukládají data správce front. K adresářům mohou být poté zpřístupněny pouze členové určené aplikační skupiny. Oprávnění ke sdílené paměti IPC systému System V používaná ke komunikaci se správcem front jsou také upravována stejným způsobem.

Skupina aplikací je název skupiny se členy, kteří mají oprávnění k provedení následujících akcí:


- spuštění aplikací MQI
- aktualizovat všechny prostředky IPCC
- změnit obsah některých adresářů správce front

Chcete-li pro správce front použít omezený režim, postupujte takto:

- Tvůrce správce front musí být ve skupině `mqm` a ve skupině aplikací.
- ID uživatele produktu `mqm` musí být ve skupině aplikací.
- Všichni uživatelé, kteří chtějí spravovat správce front, musí být ve skupině `mqm` a ve skupině aplikací.
- Všichni uživatelé, kteří chtějí spustit aplikace IBM MQ , musí být ve skupině aplikací.

Volání `MQCONN` nebo `MQCONNX` vydané uživatelem, který se nenachází ve skupině aplikací, se nezdařilo, kód příčiny `MQRC_Q_MGR_NOT_AVAILABLE`.

Omezený režim pracuje se službou autorizace IBM MQ . Proto musíte také uživatelům udělit oprávnění pro připojení k produktu IBM MQ a k přístupu k prostředkům, které vyžadují pomocí autorizační služby produktu IBM MQ .

 Další informace o konfiguraci autorizační služby produktu IBM MQ lze najít v části [Nastavení zabezpečení v systémech Windows, SYSTÉM UNIX a Linux](#).

Omezený režim produktu IBM MQ používejte pouze v případě, že ovládací prvek poskytovaný autorizační službou neposkytuje dostatečnou izolaci prostředků správce front.

Správci prostředků XA

Použijte stránku vlastností správce front produktu XA `resource manager` z Průzkumníka IBM MQ nebo sekci `XAResourceManager` v souboru `qm.ini` , abyste určili následující informace o správcích prostředků zapojených do globálních pracovních jednotek koordinovaných správcem front.

Ručně přidejte informace o konfiguraci správce prostředků XA pro každou instanci správce prostředků, která se podílí na globálních pracovních jednotkách; nejsou zadány žádné výchozí hodnoty.

Další informace o attributech správce prostředků najdete v tématu [Koordinace databáze](#) .

Název = *název* (povinný)

Tento atribut identifikuje instanci správce prostředků.

Hodnota Name může být dlouhá až 31 znaků. Můžete použít název správce prostředků, jak je definován ve své struktuře XA-switch. Pokud však používáte více než jednu instanci téhož správce prostředků, je nutné pro každou instanci vytvořit jedinečný název. Jedinečnost je možné zajistit zahrnutím názvu databáze do řetězce Name , například.

IBM MQ používá hodnotu Name ve zprávách a ve výstupu příkazu `dspmqtin` .

Neměňte název instance správce prostředků nebo odstraňte její položku z informací o konfiguraci poté, co je přidružený správce front spuštěn a že je název správce prostředků v platnosti.

SwitchFile= *název* (povinné)

Úplný název zaváděcího souboru obsahujícího strukturu přepínačů XA správce prostředků.

Používáte-li 64bitového správce front s 32bitovými aplikacemi, měla by hodnota name obsahovat pouze základní název zaváděcího souboru obsahujícího strukturu přepínačů XA správce prostředků.

32bitový soubor bude načten do aplikace z cesty určené parametrem `ExitsDefaultPath` .

64bitový soubor bude načten do správce front z cesty určené parametrem `ExitsDefaultPath64` .

XAOpenString= *řetězec* (volitelné)

Řetězec dat, který má být předán do vstupního bodu `xa_open` správce prostředků. Obsah řetězce závisí na samotném správci prostředků. Řetězec může například identifikovat databázi, ke které má tato instance správce prostředků přístup. Další informace o definování tohoto atributu najdete v tématu:

- [Přidání konfiguračních informací správce prostředků pro produkt Db2](#)
- [Přidání konfiguračních informací správce prostředků pro Oracle](#)
- [Přidání konfiguračních informací správce prostředků pro Sybase](#)
- [Přidání konfiguračních informací správce prostředků pro produkt Informix](#)

a v dokumentaci správce prostředků vyhledejte příslušný řetězec.

XACloseString= *řetězec* (volitelné)

Řetězec dat, který má být předán do vstupního bodu `xa_close` správce prostředků. Obsah řetězce závisí na samotném správci prostředků. Další informace o definování tohoto atributu najdete v tématu:

- [Přidání konfiguračních informací správce prostředků pro produkt Db2](#)
- [Přidání konfiguračních informací správce prostředků pro Oracle](#)
- [Přidání konfiguračních informací správce prostředků pro Sybase](#)
- [Přidání konfiguračních informací správce prostředků pro produkt Informix](#)

a nahlédněte do dokumentace k databázi pro příslušný řetězec.

ThreadOfControl=THREAD | PROCESS

Tento atribut je povinný pro produkt IBM MQ for Windows. Správce front používá tuto hodnotu pro serializaci, když potřebuje volat správce prostředků z jednoho z jeho vlastních procesů s více podprocesy.

Podproces

Správce prostředků je plně *informován o podprocesu*. Ve vícevláknovém procesu produktu IBM MQ lze volání funkce XA provést pro externího správce prostředků z více podprocesů současně.

PROCESS

Správce prostředků není *bezpečný pro podproces*. V procesu IBM MQ s podporou podprocesů lze ve správci prostředků provést pouze jedno volání funkce XA v daném okamžiku.

Položka `ThreadOfControl` se nevztahuje na volání funkcí XA vydaná správcem front v procesu aplikace s podporou podprocesů. Obecně platí, že aplikace, která má souběžné jednotky práce na různých podprocesech, vyžaduje, aby tento režim operace byl podporován každým správcem prostředků.

Atributy sekce kanálů

Tyto atributy určují konfiguraci kanálu.

Tyto informace se nevztahují na IBM MQ pro platformu z/OS .

Chcete-li zadat informace o kanálech, použijte stránku vlastností správce front produktu Channels z Průzkumníka IBM MQ nebo stanzu CHANNELS v souboru qm.ini .

MaxChannels= 100 | číslo

Maximální povolený počet *aktuálních* kanálů.

Hodnota musí být v rozsahu 1-65535. Výchozí hodnota je 100.

MaxActiveChannels = hodnota MaxChannels_value

Maximální počet kanálů povolených pro *aktivní* kdykoli. Výchozí hodnota je extrahována z atributu MaxChannels.

MaxInitiators= 3 | číslo

Maximální počet inicializátorů. Výchozí a současně maximální hodnota je 3.

MQIBindType= FASTPATH | STANDARD

Vazba pro aplikace:

Rychlý

Kanály se připojují pomocí rozhraní MQCONNX FASTPATH; neexistuje žádný proces agenta.

STANDARD

Kanály se připojují pomocí STANDARD.

PipeLineDélka = 1 | číslo

Maximální počet souběžných podprocesů, které kanál použije. Výchozí hodnota je 1. S každou hodnotou větší než 1 se zachází jako s hodnotou 2.

Použijete-li příkaz pipeling, nakonfigurujte správce front na obou koncích kanálu tak, aby měl hodnotu *PipeLineLength* větší než 1.

Poznámka: Potrubování je efektivní pouze pro kanály TCP/IP.

AdoptNewMCA= NO | SVR | SDR | RCVR | CLUSRCVR | ALL | FASTPATH

Pokud produkt IBM MQ obdrží požadavek na spuštění kanálu, ale zjistí, že instance kanálu je již spuštěna, v některých případech musí být stávající instance kanálu zastavena dříve, než se může nový spustit. Atribut *AdoptNewMCA* umožňuje řídit, které typy kanálů lze v tomto směru ukončit.

Pokud zadáte atribut *AdoptNewMCA* pro konkrétní typ kanálu, ale nový kanál se nespustí, protože odpovídající instance kanálu je již spuštěna:

1. Nový kanál se pokouší zastavit předchozí kanál tak, že jej bude požadovat, aby skončil.
2. Pokud předchozí kanál neodpoví na tento požadavek po uplynutí intervalu čekání *AdoptNewMCATimeout*, bude podproces nebo proces pro předchozí kanál serveru ukončen.
3. Pokud předchozí server kanálů nebyl ukončen po kroku 2 a poté, co vyprší interval čekání *AdoptNewMCATimeout* podruhé, produkt IBM MQ ukončí kanál s chybou CHANNEL IN USE .

Funkce *MCA AdoptNewse* používá pro kanály serveru, odesílatele, příjemce a příjemce klastru. V případě odesílatele nebo kanálu serveru může být v přijímajícím správci front spuštěn pouze jedna instance kanálu s konkrétním názvem. V případě přijímacího nebo přijímacího kanálu klastru může být v přijímajícím správci front spuštěn více instancí kanálu s konkrétním názvem, ale v daném okamžiku může být spuštěna pouze jedna instance určitého vzdáleného správce front.

Poznámka: Volba *AdoptNewMCA* není podporována pro kanály připojení klienta nebo serveru.

Uvedte jednu nebo více hodnot, oddělených čárkami nebo mezerami, z následujícího seznamu:

NO

Funkce *AdoptNewMCA* není povinná. Toto nastavení je výchozí.

SVR

Převzetí kanálů serveru.

SDR

Převzetí odesílacích kanálů.

RCVR

Převzetí přijímacích kanálů.

CLUSRCVR

Převzetí přijímacích kanálů klastru.

ALL

Přijmout všechny typy kanálů kromě kanálů FASTPATH.

Rychlý

Převzetí kanálu v případě, že se jedná o kanál FASTPATH. K tomu dojde pouze v případě, že je zadán také vhodný typ kanálu, například: AdoptNewMCA=RCVR, SVR, FASTPATH.

Pozor!: Atribut MCA AdoptNewse může chovat nepředvídatelně s kanály FASTPATH. Dávejte si velkou opatrnost při povolování atributu MCA AdoptNewpro kanály FASTPATH.

AdoptNewMCATimeout= 60 | 1-3600

Doba (v sekundách), po kterou bude nová instance kanálu čekat na ukončení staré instance kanálu. Uveďte hodnotu v rozsahu 1-3600. Výchozí hodnota je 60.

AdoptNewMCACheck = QM | ADDRESS | NAME | ALL

Typ kontroly požadovaný při povolení atributu AdoptNewMCA. Je-li to možné, proveďte úplnou kontrolu, abyste ochránili své kanály před vypnutím, neúmyslně nebo neúmyslně. Přinejmenším zkontrolujte, zda se názvy kanálů shodují.

Uveďte jednu nebo více z následujících hodnot oddělených čárkami nebo mezerami v případě QM, NAME nebo ALL:

QM

Zkontrolujte, zda se názvy správců front shodují.

Všimněte si, že samotné jméno správce front se shoduje, nikoli QMID.

ADDRESS

Zkontrolujte adresu IP zdroje komunikací. Například adresa TCP/IP.

Poznámka: Hodnoty CONNAME oddělené čárkou se použijí na cílové adresy, a proto nejsou pro tuto volbu důležité.

V případě, že správce front s více instancemi z produktu hosta do produktu hostb selže, budou všechny odchozí kanály tohoto správce front používat zdrojovou adresu IP produktu hostb. Pokud se liší od hosta, pak se AdoptNewMCACheck=ADDRESS nebude shodovat.

Můžete použít SSL nebo TLS se vzájemným ověřením, abyste zabránili útočníkovi, aby narušil existující běžící kanál. Případně použijte k maskování zdrojové adresy IP řešení typu HACMP s přejímací IP namísto správců front s více instancemi, nebo použijte prostředek pro rozložení zátěže sítě.

NAME

Zkontrolujte, zda se názvy kanálů shodují.

ALL

Zkontrolujte, zda jsou odpovídající názvy správců front, komunikační adresa a odpovídající názvy kanálů.

Výchozí hodnota je AdoptNewMCACheck=NAME, ADDRESS, QM.

V 8.0.0.5 ChlauthEarlyAdopt=Y |N |E

Když použijete parametr **ADOPTCTX(YES)** na objektu ověřovacích informací, kontext zabezpečení se nastaví jako ID uživatele, které je prezentováno ve struktuře MQCSP, je-li ověřeno heslem.

V takovém případě nelze přijmout další kontext zabezpečení, pokud nenastavíte parametr **ChlauthEarlyAdopt**.

Platné hodnoty pro **ChlauthEarlyAdopt** jsou tyto hodnoty:

Y

Kanál ověřuje a přebírá pověření ID uživatele a hesla, která byla poskytnuta aplikací používající ověření připojení správce front, před použitím pravidel pro ověřování kanálu. V tomto režimu provozu se pravidla ověřování kanálu shodují s ID uživatele, které je výsledkem kontrol ověření připojení.

N

Kanál zpožďuje ověření připojení pomocí pověření ID uživatele a hesla, které byly zadány aplikací, dokud nebyla použita pravidla ověření kanálu. Všimněte si, že v tomto režimu provozu, blokování ověření kanálu a pravidla mapování nemohou brát v úvahu výsledky ID uživatele a ověření platnosti hesla.

E

V 8.0.0.5 Pokud je v produktu IBM MQ 8.0.0, opravná sada Fix Pack 5 povoleno ukončení zabezpečení pro kanál, umožněte při použití parametru **ADOPTCTX(YES)** v objektu ověřovacích informací přijetí jiného kontextu zabezpečení. Použijete-li tuto hodnotu, když se uživatelské procedury zabezpečení nepoužívají, je tato hodnota stejná jako Y.

V 8.0.0.7 V produktu IBM MQ 8.0.0, opravná sada Fix Pack 7 je chování stejné jako hodnota Y.

Například výchozí objekt ověřovacích informací je nastaven na **ADOPTCTX(YES)** a uživatel fred je přihlášen. Jsou nakonfigurovány následující dvě pravidla CHLAUTH:

```
SET CHLAUTH('MY.CHLAUTH') TYPE(ADDRESSMAP) DESCR('Block all access by
default') ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
SET CHLAUTH('MY.CHLAUTH') TYPE(USERMAP) DESCR('Allow user bob and force
CONNAUTH') CLNTUSER('bob') CHCKCLNT(REQUIRED) USERSRC(CHANNEL)
```

Je zadán následující příkaz se záměrem provést ověření příkazu jako schválený kontext zabezpečení uživatele bob:

```
runmqsc -c -u bob QMGR
```

Ve skutečnosti správce front používá kontext zabezpečení produktu fred, nikoli produktu bob, a připojení se nezdaří.

Chcete-li použít kontext zabezpečení produktu bob, produkt **ChlauthEarlyAdopt** musí být nastaven na hodnotu Y.

PasswordProtection = Kompatibilní | vždy | volitelné

V produktu IBM MQ 8.0 nastavte chráněná hesla ve struktuře MQCSP místo použití SSL nebo TLS.

Ochrana heslem MQCSP je užitečná pro účely testování a vývoje, protože použití ochrany heslem MQCSP je jednodušší než nastavení šifrování SSL/TLS, ale ne jako zabezpečení.

Další informace naleznete v tématu [Ochrana heslem MQCSP](#).

ChlauthIssueVarovat = y

Nastavte tento atribut, pokud chcete, aby byla zpráva AMQ9787 generována při nastavení atributu **WARN = YES** v příkazu SET CHLAUTH.

Související pojmy

[“Stavy kanálů” na stránce 154](#)

Kanál může být v libovolném okamžiku v některém z mnoha stavů. Některé stavy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

TCP, LU62a NETBIOS

Chcete-li zadat parametry konfigurace síťového protokolu, použijte tyto stránky vlastností správce front nebo oddíly v souboru qm.ini. Přepisují výchozí atributy pro kanály.

TCP

Pomocí stránky vlastností správce front produktu TCP z Průzkumníka IBM MQ nebo stanzy TCP v souboru qm.ini zadejte konfigurační parametry protokolu Transmission Control Protocol/Internet Protocol (TCP/IP).

Port = 1414 | číslo_portu

Výchozí číslo portu pro relace TCP/IP v desítkové notaci. *dobře známé* číslo portu pro IBM MQ je 1414.

Library1= DLLName1 (pouze IBM MQ for Windows)

Název knihovny DLL soketů TCP/IP.

Výchozí hodnota je WSOCK32.

KeepAlive= NO |YES

Vypněte funkci KeepAlive zapnutou nebo vypnutou. KeepAlive=ANO způsobí, že TCP/IP pravidelně kontroluje, zda je druhý konec připojení stále dostupný. Není-li tomu tak, kanál je uzavřen.

ListenerBacklog= číslo

Přepsat výchozí počet nevyřízených požadavků pro modul listener protokolu TCP/IP.

Při příjmu v protokolu TCP/IP je nastaven maximální počet neprovedených požadavků na připojení. To může být považováno za nevyřízené požadavky požadavků čekajících na port TCP/IP pro modul listener, aby přijal požadavek. Výchozí hodnoty nevyřízených požadavků listeneru jsou zobrazeny v Tabulka 13 na stránce 116.

Tabulka 13. Výchozí nevyřízené požadavky na připojení (TCP)	
Platforma	Výchozí hodnota ListenerBacklog
Server Windows	100
Windows Pracovní stanice	5
Linux	100
Solaris	100
HP-UX	20
AIX V5.3 nebo pozdější	100

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí zobrazená hodnota. Použijte k tomu, abyste se vyvarovali dosažení limitu připojení.

A naopak, některé operační systémy mohou omezit velikost nevyřízených požadavků TCP, takže efektivní nevyřízené požadavky TCP by mohly být menší, než se zde požadovalo.

Pokud se nahromadění nevyřízených požadavků dosáhne hodnot zobrazených v Tabulka 13 na stránce 116, je připojení TCP/IP zamítnuto a kanál nelze spustit. V případě kanálů pro zprávy se tyto výsledky ve kanálu přejdou do stavu ZOPAKOVÁNÍ a později se znovu pokusí o připojení. V případě připojení klienta obdrží klient kód příčiny MQRC_Q_MGR_NOT_AVAILABLE z MQCONN a později se znovu pokusí o připojení.

Následující skupinu vlastností lze použít k řízení velikosti vyrovnávacích pamětí používaných TCP/IP. Hodnoty jsou předávány přímo do vrstvy TCP/IP operačního systému. Při používání těchto vlastností je třeba věnovat velkou pozornost. Jsou-li hodnoty nastaveny nesprávně, může to nepříznivě ovlivnit výkon TCP/IP. Další informace o tom, jak to ovlivní výkon, najdete v dokumentaci TCP/IP pro vaše prostředí. Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, a to na rozdíl od velikosti vyrovnávací paměti, které jsou opraveny produktem IBM MQ.

Connect_Timeout= 0 |number

Počet sekund před pokusem o připojení k vypršení časového limitu soketu. Výchozí hodnota nula určuje, že časový limit připojení neexistuje.

Proces kanálu produktu IBM MQ se připojuje přes neblokující sokety. Pokud tedy druhý konec zásuvky není připraven, funkce connect () se vrátí okamžitě s hodnotou EINPROGRESS nebo EWOULDBLOCK . Po této operaci bude pokus o připojení znovu proveden až do celkového počtu 20 takových pokusů, je-li hlášena chyba komunikace.

Je-li parametr `Connect_Timeout` nastaven na jinou hodnotu než nula, produkt IBM MQ čeká na určené období prostřednictvím volání `select ()`, aby se mohl soket připravit. Tím se zvyšuje šance na úspěch následného volání `connect ()`. Tato volba může být užitečná v situacích, kdy by připojení vyžadovalo určité čekací období kvůli vysokému zatížení na síti.

SndBuffVelikost=číslo | 0

Velikost odesílací vyrovnávací paměti TCP/IP použité odesílajícím koncem kanálů v bajtech. Tato hodnota stanzy může být přepsána oddílem specifičtější pro daný typ kanálu, například `RcvSndBuffSize`. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

distributed V produktu Verze 8.0 jsou noví správci front automaticky vytvářeni s výchozím nastavením 0 (viz [“Konfigurační soubory správce front qm.ini”](#) na stránce 84).

RcvBuffVelikost=číslo | 0

Velikost vyrovnávací paměti pro příjem TCP/IP používaného přijímajícím koncem kanálů, v bajtech. Tato hodnota stanzy může být přepsána oddílem specifičtější pro typ kanálu, například `RcvRcvBuffSize`. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

distributed V produktu Verze 8.0 jsou noví správci front automaticky vytvářeni s výchozím nastavením 0 (viz [“Konfigurační soubory správce front qm.ini”](#) na stránce 84).

RcvSndBuffSize= číslo | 0

Velikost vyrovnávací paměti pro odesílání protokolu TCP/IP v bajtech použitá odesílacím koncem přijímacího kanálu. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

distributed V produktu Verze 8.0 jsou noví správci front automaticky vytvářeni s výchozím nastavením 0 (viz [“Konfigurační soubory správce front qm.ini”](#) na stránce 84).

RcvRcvBuffSize= číslo | 0

Velikost vyrovnávací paměti pro příjem TCP/IP používaného přijímajícím koncem kanálu příjemce, v bajtech. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

distributed V produktu Verze 8.0 jsou noví správci front automaticky vytvářeni s výchozím nastavením 0 (viz [“Konfigurační soubory správce front qm.ini”](#) na stránce 84).

SvrSndBuffSize= číslo | 0

Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá na konci serveru pro kanál připojení serveru připojení klienta. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

distributed V produktu Verze 8.0 jsou noví správci front automaticky vytvářeni s výchozím nastavením 0 (viz [“Konfigurační soubory správce front qm.ini”](#) na stránce 84).

SvrRcvBuffSize= číslo | 0

Velikost vyrovnávací paměti pro příjem protokolu TCP/IP v bajtech použitá na konci serveru kanálu připojení klienta pro připojení klienta k serveru. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

distributed V produktu Verze 8.0 jsou noví správci front automaticky vytvářeni s výchozím nastavením 0 (viz [“Konfigurační soubory správce front qm.ini”](#) na stránce 84).

Windows LU62 (pouze IBM MQ for Windows)

Použijte stránku vlastností správce front produktu LU6.2 z Průzkumníka IBM MQ nebo sekci LU62 v souboru `qm.ini`, abyste určili parametry konfigurace protokolu SNA LU 6.2.

TPName

Název transakčního programu, který má být spuštěn na vzdáleném serveru.

Library1= DLLName 1

Název knihovny APPC DLL.

Výchozí hodnota je WCPIC32.

Library2= DLLName2

Totéž jako Library1, používá se, pokud je kód uložen ve dvou samostatných knihovnách.

Výchozí hodnota je WCPIC32.

Windows NETBIOS (pouze systém IBM MQ for Windows)

Použijte stránku vlastností správce front produktu Netbios z Průzkumníka IBM MQ nebo stanzy NETBIOS v souboru qm.ini , abyste určili parametry konfigurace protokolu NetBIOS .

LocalName= *název*

Název, pod kterým je tento počítač znám v síti LAN.

AdapterNum= 0 | *adaptér_adaptéru*

Číslo adaptéru sítě LAN. Výchozí je adaptér 0.

NumSess= 1 | *počet_relací*

Počet relací k přidělení. Výchozí hodnota je 1.

NumCmds= 1 | *počet_příkazů*

Počet příkazů k přidělení. Výchozí hodnota je 1.

NumNames= 1 | *počet_názevů*

Počet názvů, které se mají přidělit. Výchozí hodnota je 1.

Library1= DLLName1

Název knihovny DLL NetBIOS .

Výchozí hodnota je NETAPI32.

Windows SPX (pouze IBM MQ for Windows)

Použijte stránku vlastností správce front produktu SPX z Průzkumníka IBM MQ nebo sekci SPX v souboru qm.ini , abyste mohli zadat parametry konfigurace protokolu SPX.

Socket = 5E86 | *číslo_soketu*

Číslo soketu SPX v hexadecimální notaci. Výchozí hodnota je X'5E86'.

BoardNum= 0 | *adaptér_adaptéru*

Číslo adaptéru LAN. Výchozí je adaptér 0.

KeepAlive= NE | ANO

Vypněte funkci KeepAlive zapnutou nebo vypnutou.

Volba KeepAlive=YES způsobí, že SPX pravidelně kontroluje, zda je druhý konec připojení stále dostupný. Není-li tomu tak, kanál je uzavřen.

Library1= DLLName1

Název knihovny SPX DLL.

Výchozí hodnota je WSOCK32.DLL.

Library2= DLLName2

To samé jako LibraryName1, použito, pokud je kód uložen ve dvou samostatných knihovnách.

Výchozí hodnota je WSOCK32.DLL.

ListenerBacklog= číslo

Potlačit výchozí počet nevyřízených požadavků pro modul listener SPX.

Při příjmu na SPX je nastaven maximální počet neprovedených požadavků na připojení. Tento stav lze považovat za seznam požadavků čekajících na soket protokolu SPX pro příjem požadavků, které čekají na příjem požadavku. Výchozí hodnoty nevyřízených požadavků listeneru jsou zobrazeny v [Tabulka 14 na stránce 119](#).

Tabulka 14. Výchozí nevyřízené požadavky na připojení (SPX)	
Platforma	Výchozí hodnota ListenerBacklog
Server Windows	100
Windows Pracovní stanice	5

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí zobrazená hodnota. Použijte k tomu, abyste se vyvarovali dosažení limitu připojení.

Naopak, některé operační systémy mohou omezit velikost nevyřízených požadavků SPX, takže efektivní nevyřízené požadavky SPX by mohly být menší, než se zde požadovalo.

Pokud počet nevyřízených požadavků dosáhne hodnot zobrazených v Tabulka 14 na stránce 119, je spojení SPX odmítnuto a kanál nelze spustit. V případě kanálů pro zprávy se tyto výsledky ve kanálu přejdou do stavu ZOPAKOVÁNÍ a později se znovu pokusí o připojení. V případě připojení klienta obdrží klient kód příčiny MQRC_Q_MGR_NOT_AVAILABLE z produktu MQCONN a měl by pokus o připojení zopakovat později.

Cesta k uživatelské proceduře

Pomocí stránky vlastností správce front produktu Exits z Průzkumníka IBM MQ nebo stanzy ExitPath v souboru qm.ini zadejte cestu k uživatelským ukončovacím programům v systému správce front.

ExitsDefaultCesta = řetězec

Atribut Cesta ExitsDefaultuvádí umístění:

- 32bitový kanál se ukončí pro klienty
- 32bitový kanál se ukončí a pro servery existují ukončení konverze dat
- Nekvalifikované soubory načtení přepínače XA

ExitsDefaultPath64= řetězec

Atribut ExitsDefaultPath64 uvádí umístění:

- Běžné uživatelské procedury kanálu pro klienty
- Běžné uživatelské procedury kanálu a uživatelské procedury pro převod dat pro servery
- Nekvalifikované soubory načtení přepínače XA

Uživatelské procedury rozhraní API

Pro server použijte stránku vlastností správce front produktu Exits z objektu MQ Explorernebo oddíl ApiExitLocal v souboru qm.ini pro identifikaci uživatelských procedur rozhraní API pro správce front. V případě klienta změňte sekci ApiExitLocal v souboru mqclient.ini k identifikaci uživatelských procedur rozhraní API pro správce front.

V systémech Windows můžete také pomocí příkazu amqmdain změnit položky pro ukončení rozhraní API. (Chcete-li identifikovat rutiny ukončení rozhraní API pro všechny správce front, použijte oddíl ApiExitCommon a ApiExitTemplate , jak je popsáno v tématu [“Uživatelské procedury rozhraní API”](#) na stránce 103.)

Všimněte si, že má-li uživatelská procedura rozhraní API pracovat správně, musí být zpráva ze serveru odeslána klientovi, která není konvertována. Poté, co uživatelská procedura rozhraní API zpracuje zprávu, musí být zpráva převedena na klienta. Proto je třeba, abyste instalovali všechny uživatelské procedury pro převod na klientovi.

Úplný popis atributů těchto stanz naleznete v tématu [Konfigurace uživatelských procedur rozhraní API](#).

stanza QMErrorLog na systému SYSTÉM UNIX, Linuxa Okna

Pomocí stránky vlastností správce front produktu Extended z MQ Explorernebo ze stanzy QMErrorLog v souboru qm.ini můžete přizpůsobit operaci a obsah protokolů chyb správce front.



Upozornění: K provedení změn můžete použít produkt MQ Explorer pouze v případě, že používáte lokálního správce front na platformě Windows .

ErrorLogVelikost = maxsize

Uvádí velikost protokolu chyb správce front, ve kterém je kopírován do zálohování. Hodnota *maxsize* musí být v rozsahu 32768 až 2147483648 bajtů. Není-li parametr `ErrorLogSize` zadán, bude použita výchozí hodnota 2097152 bajtů (2 MB).

ExcludeMessage= msgIds

Určuje zprávy, které nemají být zapsány do protokolu chyb správce front. Je-li systém IBM MQ intenzivně využíván, je při zastavování a spouštění mnoha kanálů odesláno velké množství informačních zpráv do konzoly z/OS a do protokolu hardcopy. Most produktu IBM MQ - IMS a správce vyrovnávacích paměti mohou také produkovat velké množství informačních zpráv, takže vyloučení zpráv vám zabrání v přijetí velkého počtu zpráv, pokud jej požadujete. *msgIds* obsahují seznam ID zprávy oddělený čárkami:

5211-Byla překročena maximální délka názvu vlastnosti.
5973-Odběr distribuovaného publikování/odběru je blokován
5974-Publikování distribuovaného publikování/odběru blokováno.
6254-Systému se nepodařilo dynamicky načíst sdílenou knihovnu.
IBM i 7163 - Zpráva o spuštění úlohy (pouze IBM i).
7234 - Počet načtených zpráv.
9001 - Program kanálu byl standardně ukončen.
9002 - Program kanálu byl spuštěn.
9202 - Vzdálený hostitel je nedostupný.
9208-Chyba při příjmu z hostitele
9209-Připojení bylo ukončeno.
9228-Nelze spustit odpovídací modul kanálu
9489-Překročen maximální počet instancí SVRCONN
9490-Překročen maximální počet instancí SVRCONN na klienta
9508-Nelze se připojit ke správci front
9524 - Vzdálený správce front je nedostupný.
9528 - Zavření kanálu vyžadované uživatelem.
9545-Platnost intervalu odpojení vypršela
9558-Vzdálený kanál není k dispozici
9637-Kanálu chybí certifikát
9776-Kanál byl blokován ID uživatele
9777-Kanál NOACCESS byl blokován kanálem.
9782-Spojení bylo blokováno adresou
9999 - Program kanálu byl ukončen nestandardně.

SuppressMessage= msgIds

Určuje zprávy, které jsou zapsány do protokolu chyb správce front pouze jednou za určený časový interval. Je-li systém IBM MQ intenzivně využíván, je při zastavování a spouštění mnoha kanálů odesláno velké množství informačních zpráv do konzoly z/OS a do protokolu hardcopy. Most IBM MQ - IMS a správce vyrovnávací paměti mohou také produkovat velké množství informačních zpráv, takže potlačení zpráv vám zabrání v příjmu několika opakujících se zpráv, pokud to požadujete. Časový interval je určen parametrem `SuppressInterval` . *msgIds* obsahují seznam ID zprávy oddělený čárkami:

5211-Byla překročena maximální délka názvu vlastnosti.
5973-Odběr distribuovaného publikování/odběru je blokován
5974-Publikování distribuovaného publikování/odběru blokováno.
6254-Systému se nepodařilo dynamicky načíst sdílenou knihovnu.
IBM i 7163 - Zpráva o spuštění úlohy (pouze IBM i).
7234 - Počet načtených zpráv.

9001 - Program kanálu byl standardně ukončen.
9002 - Program kanálu byl spuštěn.
9202 - Vzdálený hostitel je nedostupný.
9208-Chyba při příjmu z hostitele
9209-Připojení bylo ukončeno.
9228-Nelze spustit odpovídací modul kanálu
9489-Překročen maximální počet instancí SVRCONN
9490-Překročen maximální počet instancí SVRCONN na klienta
9508-Nelze se připojit ke správci front
9524 - Vzdálený správce front je nedostupný.
9528 - Zavření kanálu vyžadované uživatelem.
9545-Platnost intervalu odpojení vypršela
9558-Vzdálený kanál není k dispozici
9637-Kanálu chybí certifikát
9776-Kanál byl blokován ID uživatele
9777-Kanál NOACCESS byl blokován kanálem.
9782-Spojení bylo blokováno adresou
9999 - Program kanálu byl ukončen nestandardně.

Je-li v obou SuppressMessage a ExcludeMessage uvedeno stejné ID zprávy, tato zpráva je vyloučena.

SuppressInterval= délka

Určuje časový interval v sekundách, ve kterém jsou zprávy zadané v SuppressMessage zapsány do protokolu chyb správce front pouze jednou. *délka* musí být v rozsahu 1 až 86400 sekund. Není-li parametr SuppressInterval zadán, použije se výchozí hodnota 30 sekund.

Výchozí typ vazby správce front

Použijte stránku vlastností správce front produktu Extended z Průzkumníka IBM MQ nebo stanzu Connection v souboru qm.ini , abyste určili výchozí typ vazby. Všimněte si, že musíte vytvořit sekci Connection , pokud ji potřebujete.

DefaultBindTyp = SHARED | ISOLATED

Je-li vlastnost DefaultBindnastavena na hodnotu ISOLATED, jsou aplikace a správce front spouštěny v samostatných procesech a mezi nimi nejsou sdíleny žádné prostředky.

Je-li typ DefaultBindnastaven na hodnotu SHARED, jsou aplikace a správce front spouštěny v oddělených procesech, ale některé prostředky jsou mezi nimi sdíleny.

Výchozí hodnota je SHARED.



Upozornění: DefaultBindType se vztahuje na všechna volání MQCONN a všechny s použitím MQCONNX s parametrem MQCNO_STANDARD_BINDING.

Změna **DefaultBindType** může způsobit snížení výkonu některých aplikací.

Sekce SSL a TLS konfiguračního souboru správce front

Použijte sekci SSL konfiguračního souboru správce front pro konfiguraci kanálů SSL nebo TLS ve správci front.

Protokol OCSP (Online Certificate Status Protocol)

Certifikát může obsahovat rozšíření AuthorityInfoAccess. Toto rozšíření určuje server, který má být kontaktován prostřednictvím protokolu OCSP (Online Certificate Status Protocol). Chcete-li povolit zabezpečení SSL nebo TLS ve správci front pro použití rozšíření AuthorityInfoAccess, ujistěte se, že je server OCSP uvedený v nich dostupný, správně nakonfigurovaný a že je přístupný po síti. Další informace naleznete v tématu Práce s odvolanými certifikáty.

CrlDistributionPoint (CDP)

Certifikát může obsahovat příponu CrlDistributionPoint. Toto rozšíření obsahuje adresu URL, která identifikuje protokol použitý ke stažení seznamu zrušených certifikátů (CRL) a také server, který má být kontaktován.

Chcete-li povolit použití zabezpečení SSL nebo TLS ve správci front pro použití rozšíření CrlDistributionPoint, ujistěte se, že je server CDP uvedený v nich dostupný, správně nakonfigurovaný a přístupný po síti.

Sekce SSL

Použijte sekci SSL v souboru `qm.ini` a nakonfigurujte, jak se kanály SSL nebo TLS ve vašem správci front pokusí použít následující zařízení, a jak budou reagovat, pokud se při použití vyskytnou problémy.

V každém z následujících případů, pokud uvedená hodnota není jedna z uvedených platných hodnot, pak se použije výchozí hodnota. Nezapíše se žádné chybové zprávy, které uvádějí, že je uvedena neplatná hodnota.

CDPCheckExtensions= YES | NO

CDPCheckExtensions uvádí, zda se kanály SSL nebo TLS v tomto správci front pokouší zkontrolovat servery CDP, které jsou pojmenované v rozšířeních certifikátu bodu CrlDistributionPoint.

- AN0: Kanály SSL nebo TLS se snaží zkontrolovat servery CDP za účelem určení, zda je digitální certifikát odvolán.
- N0: Kanály SSL nebo TLS se nesnažte kontrolovat servery CDP. Tato hodnota je výchozí.

OCSPAAuthentication= REQUIRED | WARN | OPTIONAL

OCSPAAuthentication určuje akci, která má být provedena, když nelze zjistit stav odvolání ze serveru OCSP.

Je-li povolena kontrola OCSP, pokusí se kanál zabezpečení SSL nebo TLS kontaktovat server OCSP.

Není-li program kanálu schopen kontaktovat žádné servery OCSP nebo pokud žádný server nemůže poskytnout stav odvolání certifikátu, použije se hodnota parametru OCSPAAuthentication.

- REQUIRED: Selhání při zjišťování stavu odvolání způsobí, že připojení bude uzavřeno s chybou. Tato hodnota je výchozí.
- WARN: Selhání při zjišťování stavu odvolání způsobí zapsání varovné zprávy do protokolu chyb správce front, ale připojení je povoleno pokračovat.
- VOLITELNÉ: Selhání při určování stavu odvolání umožňuje bezobslužně pokračovat v připojení. Neuvádí se žádná varování nebo chyby.

OCSPCheckExtensions= YES | NO

OCSPCheckExtensions uvádí, zda se kanály SSL a TLS v tomto správci front pokusí zkontrolovat servery OCSP, které jsou pojmenované v rozšířeních certifikátů AuthorityInfoAccess.

- AN0: Kanály SSL a TLS se snaží zkontrolovat servery OCSP, aby určily, zda je digitální certifikát odvolán. Tato hodnota je výchozí.
- N0: Kanály SSL a TLS se nepokouší o kontrolu serverů OCSP.

SSLHTTPProxyName= řetězec

Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použít pro kontroly OCSP. Za touto adresou může následovat volitelné číslo portu uzavřené v závorkách. Pokud číslo portu neurčíte, zvolí se výchozí port HTTP, který má číslo 80. Na platformách HP-UX PA-RISC a Sun Solaris SPARC a pro 32bitové klienty na systému AIX může být síťová adresa pouze adresou IPv4; na jiných platformách může být použita adresa IPv4 nebo IPv6.

Tento atribut může být nezbytný, pokud například ochranná bariéra brání přístupu k adrese URL odpovídajícího modulu OCSP.

Vlastnosti uživatelské procedury

Chcete-li zadat informace o vlastnostech ukončení ve správci front, použijte stránku vlastností správce front klastru z konzoly MQ Explorernebo lokální sekci ExitPropertiesv souboru qm.ini . Případně ji můžete nastavit pomocí příkazu **amqmdain** .

Standardně je toto nastavení zděděno z atributu CLWLMode ve stanze ExitProperties v konfiguraci celého počítače (popsané v části “Vlastnosti uživatelské procedury” na stránce 100). Změňte toto nastavení pouze v případě, že chcete tohoto správce front nakonfigurovat jiným způsobem. Tuto hodnotu lze u jednotlivých správců front přepsat s použitím atributu režimu pracovní zátěže klastru na stránce vlastností správce front klastru.

CLWLMode= SAFE | FAST

Ukončení pracovní zátěže klastru (CLWL) vám umožňuje určit, která fronta klastru v klastru má být otevřena v rámci odezvy na volání MQI (například MQOPEN , MQPUT). Uživatelská procedura CLWL se spustí buď v režimu FAST, nebo v režimu SAFE, v závislosti na hodnotě, kterou zadáte v atributu CLWLMode. Pokud vynecháte atribut CLWLMode, uživatelská procedura pracovní zátěže klastru se spustí v režimu SAFE.

SAFE

Spustíte uživatelskou proceduru CLWL v odděleném procesu od správce front. Toto nastavení je výchozí.

Pokud se vyskytne problém s uživatelskou procedurou CLWL, když je spuštěn v režimu SAFE, nastane následující situace:

- Proces serveru CLWL (amqzlw0) selže.
- Správce front restartuje proces serveru CLWL.
- Chyba je ohlášena v protokolu chyb. Pokud probíhá volání MQI, obdržíte oznámení ve formě návratového kódu.

Integrita správce front je zachována.

Poznámka: Spuštění uživatelské procedury CLWL v odděleném procesu může ovlivnit výkon.

FAST

Spustíte uživatelskou proceduru klastru vloženou do procesu správce front.

Zadáním této volby zvýšíte výkon tím, že se vyhnete nákladům na přepínání procesu, které jsou přidruženy ke spuštění v režimu SAFE, ale provádí se tak na úkor integrity správce front. Ukončení CLWL byste měli spustit pouze v režimu FAST, jste-li přesvědčeni, že při ukončení CLWL nejsou žádné problémy s **žádným** problémem, a vy jste obzvláště znepokojeni výkonem.

Pokud se vyskytne problém, když je uživatelská procedura CLWL spuštěna v režimu FAST, správce front selže a vy spustíte riziko, že integrita správce front bude ohrožena.

Podfond

Tato stanza je vytvořena IBM MQ. Neměňte jej.

Oddíl Subpool a atribut ShortSubpoolNázev v rámci této stanzy jsou automaticky zapisovány produktem IBM MQ při vytváření správce front. Produkt IBM MQ zvolí hodnotu pro název ShortSubpool. Tuto hodnotu neměňte.

Název odpovídá adresáři a symbolickému odkazu vytvořenému v adresáři /var/mqm/sockets , který produkt IBM MQ používá pro vnitřní komunikaci mezi spuštěnými procesy.

Sekce systému souborů souboru qm.ini

Výchozí oprávnění nastavená u souborů protokolu chyb by měla být užitečná ve většině případů, a proto není třeba, aby je většina administrátorů produktu IBM MQ měnila.

Administrátor produktu IBM MQ však může chtít upravit oprávnění pro příslušné soubory protokolu chyb. V takovém případě by měli nastavit volbu stanice systému souborů **ValidateAuth=Ne**, která způsobí, že správce front ponechá oprávnění v nezměněné podobě poté.



Výchozí chování (bez hodnoty **ValidateAuth=Ne**) určuje, že správce front zkontroluje oprávnění k souboru protokolů chyb správce front a změny je zpět na své výchozí hodnoty. Tato kontrola může nastat kdykoli, včetně během ukončení nebo operace spuštění správce front.

Konfigurace distribuovaných front

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ, včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Před čtením této sekce je užitečné porozumět kanálům, frontám a dalším konceptům představeným v tématu [Distribuované fronty a klastry](#).

Informace v následujících odkazech použijte k připojení aplikací pomocí distribuovaných front:

- [“Jak odeslat zprávu jinému správci front”](#) na stránce 146
- [“Spouštěcí kanály”](#) na stránce 166
- [“Bezpečnost zpráv”](#) na stránce 164
- [“IBM MQ technologie distribuovaných front”](#) na stránce 124
- [“Úvod do distribuované správy front”](#) na stránce 143
-  [“Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux”](#) na stránce 173
-  [“Monitorování a řízení kanálů v systému IBM i”](#) na stránce 195

Související pojmy

[“přizpůsobení IBM MQ for z/OS”](#) na stránce 528

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ.

[“Konfigurace připojení mezi serverem a klientem”](#) na stránce 14

Chcete-li nakonfigurovat komunikační propojení mezi IBM MQ MQI clients a servery, rozhodněte se v komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

[“Změna konfiguračních informací IBM MQ a správce front”](#) na stránce 81

Změňte chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

[“Konfigurace správců front v systému z/OS”](#) na stránce 523

Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

[“Nastavení komunikace s ostatními správci front”](#) na stránce 590

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS, které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

Související úlohy

[“Konfigurace klastru správce front”](#) na stránce 216




Klastry poskytují mechanismus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

IBM MQ technologie distribuovaných front

Dílčí témata v tomto oddílu popisují techniky, které se používají při plánování kanálů. Tato dílčí témata popisují techniky, které vám pomohou naplánovat vzájemné propojení správců front a správu toku zpráv mezi vašimi aplikacemi.

Příklady plánování kanálů zpráv viz:

- [Příklad plánování kanálů zpráv pro distribuované platformy](#)

-  [Příklad plánování kanálů zpráv pro produkt IBM MQ for IBM i](#)
-  [Příklad plánování kanálů zpráv pro produkt z/OS](#)
-  [Příklad plánování kanálů zpráv pro produkt z/OS s použitím skupin sdílení front](#)

Související pojmy

“Konfigurace distribuovaných front” na stránce 124

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související informace

[Kanály](#)


[Úvod do systému front zpráv](#)

[Distribuované fronty a klastry](#)

[Příklad konfiguračních informací](#)

Řízení toku zpráv

Řízení toku zpráv je úloha, která zahrnuje nastavení a údržbu tras zpráv mezi správci front. Je důležité pro přenosové cesty, které multi-hop přes mnoho správců front. Tento oddíl popisuje použití front, definic alias front a kanálů zpráv ve vašem systému za účelem dosažení řízení toku zpráv.

Tok zpráv řídíte pomocí mnoha technik, které byly zavedeny v produktu “[Konfigurace distribuovaných front](#)” na stránce 124. Je-li správce front v klastru, je tok zpráv řízen pomocí různých technik, jak je popsáno v tématu “[řízení toku zpráv](#)” na stránce 125.  Pokud jsou správci front ve skupině sdílení front a je povoleno ukládání do front v rámci skupiny (IGQ), může být tok zpráv řízen agenty IGQ. Tito agenti jsou popsány v tématu [Řazení do front v rámci skupiny](#).

K dosažení řízení toku zpráv můžete použít následující objekty:

- Přenosové fronty
- Kanály zpráv
- Definice vzdálené fronty
- Definice aliasu správce front
- Definice alias fronty pro odpověď

Objekty správce front a fronty jsou popsány v části [Typy objektů](#). Kanály zpráv jsou popsány v tématu [Distribuované komponenty řazení do fronty](#). Následující techniky používají tyto objekty k vytvoření toků zpráv ve vašem systému:

- Vložení zpráv do vzdálených front
- Směrování podle konkrétních přenosových front
- Příjem zpráv
- Předání zpráv prostřednictvím systému
- Oddělování toků zpráv
- Přepnutí toku zpráv do jiného cíle
- Vyřešení názvu fronty pro odpověď na název aliasu

Poznámka

Všechny koncepce popsané v této sekci jsou relevantní pro všechny uzly v síti a zahrnují odesílání a příjem konců kanálů zpráv. Z tohoto důvodu je ve většině příkladů ilustrován pouze jeden uzel. Výjimka je v tom případě, že příklad vyžaduje explicitní spolupráci administrátora na druhém konci kanálu zpráv.

Dříve než budete pokračovat s jednotlivými technikami, je užitečné se znovu okapat o konceptech rozlišení názvu a o třech způsobech použití definic vzdálených front. Viz téma [Distribuované fronty a klastry](#).

Související pojmy

“Názvy front v záhlaví přenosu” na stránce 126

Názvy cílových front cestují se zprávou v záhlaví přenosu, dokud není dosažena cílová fronta.

“Jak vytvořit správce front a odpovědět na aliasy” na stránce 126

Toto téma vysvětluje tři způsoby, jak můžete vytvořit definici vzdálené fronty.

Názvy front v záhlaví přenosu

Názvy cílových front cestují se zprávou v záhlaví přenosu, dokud není dosažena cílová fronta.

Název fronty použitý aplikací, název logické fronty, je vyřešen správcem front do názvu cílové fronty. Jinými slovy, název fyzické fronty. Tento název cílové fronty se pohybuje se zprávou v samostatné datové oblasti, záhlaví přenosu, dokud není dosaženo cílové fronty. Hlavička přenosu je poté odstraněna.

Když vytváříte paralelní třídy služeb, změníte část správce front tohoto názvu fronty. Nezapomeňte vrátit název správce front k původnímu názvu, až bude dosaženo konce přesměrování třída-slужby.

Jak vytvořit správce front a odpovědět na aliasy

Toto téma vysvětluje tři způsoby, jak můžete vytvořit definici vzdálené fronty.

Objekt definice vzdálené fronty se používá třemi různými způsoby. Část [Tabulka 15](#) na stránce 127 vysvětluje, jak definovat každý ze tří způsobů:

- Použití definice vzdálené fronty k redefinování názvu lokální fronty.

Aplikace poskytuje při otevírání fronty pouze název fronty a tento název fronty je názvem definice vzdálené fronty.

Definice vzdálené fronty obsahuje názvy cílové fronty a správce front. Volitelně může definice obsahovat název přenosové fronty, která má být použita. Není-li zadán žádný název přenosové fronty, správce front použije název správce front, převzaté z definice vzdálené fronty, pro název přenosové fronty. Není-li definována přenosová fronta s tímto názvem, ale je definována výchozí přenosová fronta, použije se výchozí přenosová fronta.

- Použití definice vzdálené fronty k předefinování názvu správce front.

Aplikační program nebo program kanálu poskytuje při otevření fronty název fronty spolu s názvem vzdáleného správce front.

Pokud jste zadali definici vzdálené fronty se stejným názvem jako název správce front a vy jste v definici ponechal název fronty, nahradí správce front název správce front v otevřeném volání s názvem správce front v definici.

Kromě toho může definice obsahovat název přenosové fronty, která má být použita. Není-li zadán žádný název přenosové fronty, správce front vezme název správce front, převzato z definice vzdálené fronty, pro název přenosové fronty. Není-li definována přenosová fronta s tímto názvem, ale je definována výchozí přenosová fronta, použije se výchozí přenosová fronta.

- Použití definice vzdálené fronty k redefinování názvu fronty pro odpověď.

Pokaždé, když aplikace vloží zprávu do fronty, může poskytnout název fronty pro odpověď na zprávy odpovědi, ale s prázdnou hodnotou názvu správce front.

Zadáte-li definici vzdálené fronty se stejným názvem jako fronta pro odpověď, nahradí lokální správce front název fronty pro odpověď s názvem fronty z vaší definice.

V definici můžete zadat název správce front, nikoli však název přenosové fronty.

Tabulka 15. Tři způsoby použití objektu definice vzdálené fronty

Použití	Název správce front	Název fronty	Jméno přenosové fronty
1. Definice vzdálené fronty (při volání OPEN)			
Dodáno v rámci volání	prázdné nebo lokální QM	(*) vyžadováno	nelze použít
Dodáno v definici	povinné	povinné	volitelné
2. Alias správce front (při volání OPEN)			
Dodáno v rámci volání	(*) požadováno a nikoli lokální QM	povinné	nelze použít
Dodáno v definici	povinné	prázdná	volitelné
3. Alias fronty pro odpověď (ve volání PUT)			
Dodáno v rámci volání	prázdná	(*) vyžadováno	nelze použít
Dodáno v definici	volitelné	volitelné	prázdná

Poznámka: (*) znamená, že tento název je název objektu definice

Formální popis naleznete v tématu [Rozpoznání názvu fronty](#).

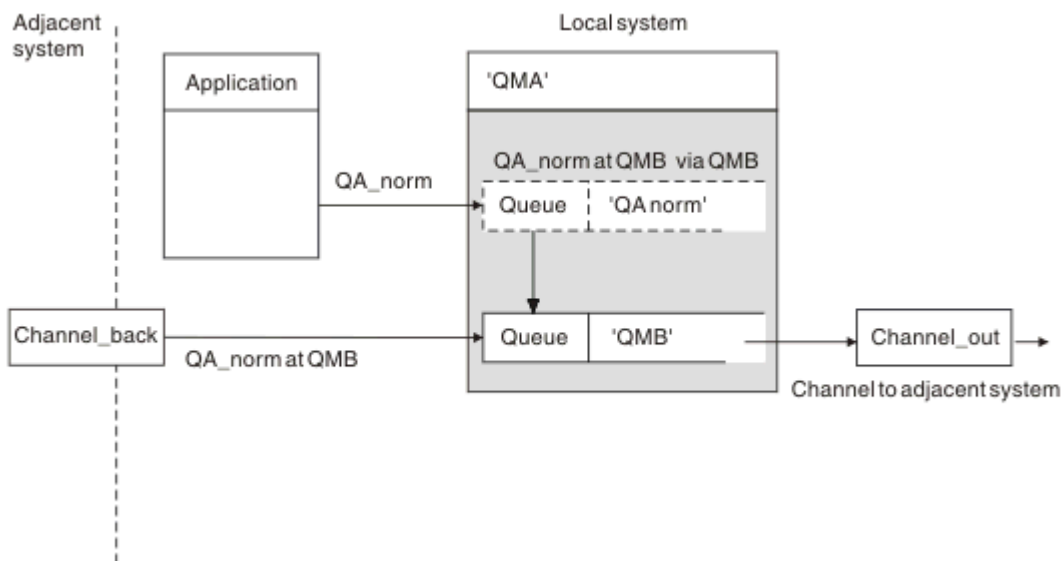
Vložení zpráv do vzdálených front

K převodu názvu fronty do přenosové fronty na sousední správce front můžete použít objekty definice vzdálené fronty.

V prostředí s distribuovanými frontami je přenosová fronta a kanál ústředním bodem pro všechny zprávy v umístění, odkud zprávy pocházejí z aplikací ve vašem lokálním systému, nebo přicházejí přes kanály ze sousedního systému. [Obrázek 6 na stránce 128](#) zobrazuje aplikaci umístění zpráv do logické fronty s názvem 'QA_norm'. Rozpoznání názvu používá definici vzdálené fronty 'QA_norm' k výběru přenosové fronty QMB. Pak přidá záhlaví přenosu do zpráv, které uvádí 'QA_norm at QMB'.

Zprávy přicházející ze sousedního systému v systému 'Channel_back' mají záhlaví přenosu s názvem fyzické fronty 'QA_norm at QMB', například. Tyto zprávy jsou nezměněny na přenosové frontě QMB.

Kanál přesune zprávy do sousedního správce front.



Obrázek 6. Definice vzdálené fronty se používá k převedení názvu fronty na přenosovou frontu do sousedního správce front.

Jste-li administrátorem systému IBM MQ , musíte:

- Definovat kanál zpráv ze sousedního systému
- Definovat kanál zpráv na sousedící systém
- Vytvoření fronty přenosových front QMB
- Definujte objekt vzdálené fronty 'QA_norm', abyste vyřešili název fronty použité aplikacemi s názvem cílové fronty, názvem správce cílové fronty a názvem přenosové fronty.

V prostředí klastrování je třeba definovat pouze kanál příjemce klastru v lokálním správci front. Frontu přenosu nebo objekt vzdálené fronty není třeba definovat. Viz [Klastry](#).

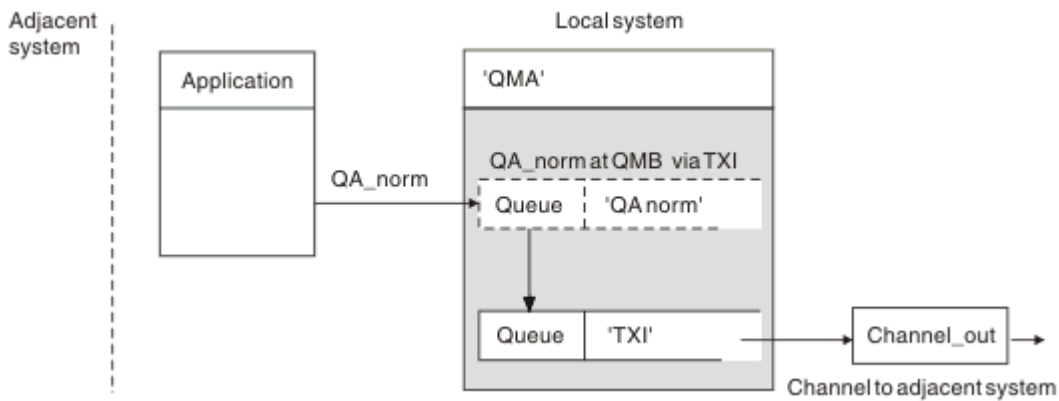
Další informace o rozlišování názvů

Efekt definice vzdálené fronty je definovat název fyzické cílové fronty a název správce front. Tyto názvy jsou vloženy do záhlaví přenosu zpráv.

Příchozí zprávy ze sousedního systému již mají tento typ rozpoznání názvu, který provedl původní správce front. Proto mají záhlaví přenosu zobrazující název fyzické cílové fronty a název správce front. Tyto zprávy nejsou ovlivněny definicemi vzdálených front.

Výběr přenosové fronty

Chcete-li povolit odesílání zpráv stejnému sousednímu správci front, můžete použít definici vzdálené fronty k tomu, abyste povolili odesílání zpráv jinou přenosovou frontu.



Obrázek 7. Definice vzdálené fronty umožňuje použití jiné přenosové fronty.

Když v prostředí rozděleném do front potřebujete změnit tok zpráv z jednoho kanálu na druhý, použijte stejnou konfiguraci systému, jak je zobrazeno v [Obrázek 6 na stránce 128](#) v [“Vložení zpráv do vzdálených front”](#) na stránce 127. [Obrázek 7 na stránce 129](#) v tomto tématu ukazuje, jak používat definici vzdálené fronty k odesílání zpráv přes jinou přenosovou frontu, a tím i přes jiný kanál, do stejného sousedního správce front.

Pro konfiguraci zobrazenou v [Obrázek 7 na stránce 129](#) musíte poskytnout objekt vzdálené fronty 'QA_norm' a přenosovou frontu 'TX1'. Musíte zadat 'QA_norm', abyste vybrali frontu 'QA_norm' ve vzdáleném správci front, přenosové frontě 'TX1' a správce front 'QMB_priority'. Určete 'TX1' v definici kanálu sousedící se systémem.

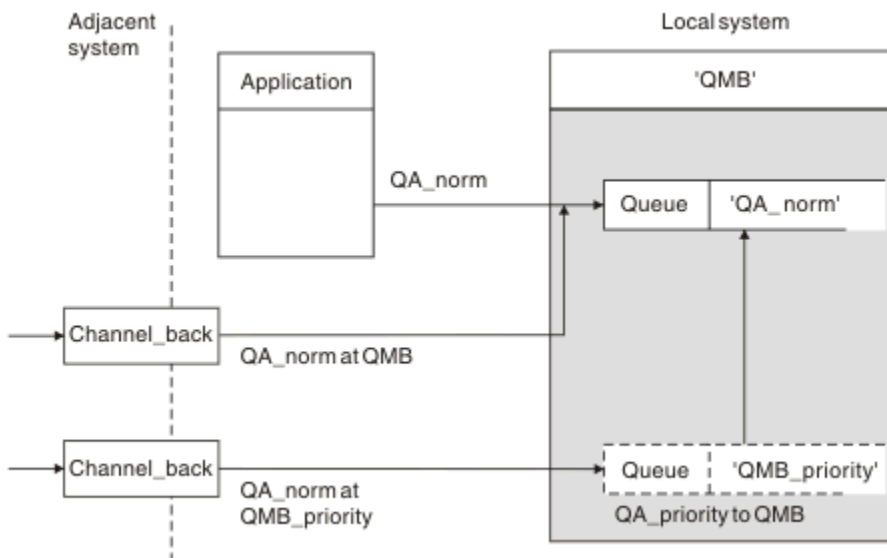
Zprávy jsou umístěny do přenosové fronty 'TX1' s hlavičkou přenosu obsahujícím 'QA_norm' při QMB_priority' a jsou posílána přes kanál na sousední systém.

Seznam kanálů byl z tohoto obrázku odstraněn, protože by potřeboval alias správce front.

V klastrovaném prostředí není třeba definovat přenosovou frontu nebo definici vzdálené fronty. Další informace viz [“Definování front klastru”](#) na stránce 217.

Příjem zpráv

Správce front je možné nakonfigurovat tak, aby přijímal zprávy od jiných správců front. Je třeba zajistit, aby nedošlo k neúmyslnému rozpoznání názvu.



Obrázek 8. Přímé přijímání zpráv a řešení názvu správce front aliasu

Stejně jako uspořádání zpráv, které mají být odeslány, musí správce systému také zajistit, aby zprávy byly přijaty ze sousedních správců front. Přijaté zprávy obsahují fyzický název cílového správce front a fronty v záhlaví přenosu. Jsou s nimi stejné jako zprávy z lokální aplikace určující název správce front i název fronty. Kvůli této léčbě byste měli zajistit, aby zprávy vstupující do vašeho systému neměly nezáměrné rozlišení jména provedeno. Tento scénář viz [Obrázek 8 na stránce 129](#).

Pro tuto konfiguraci musíte připravit:

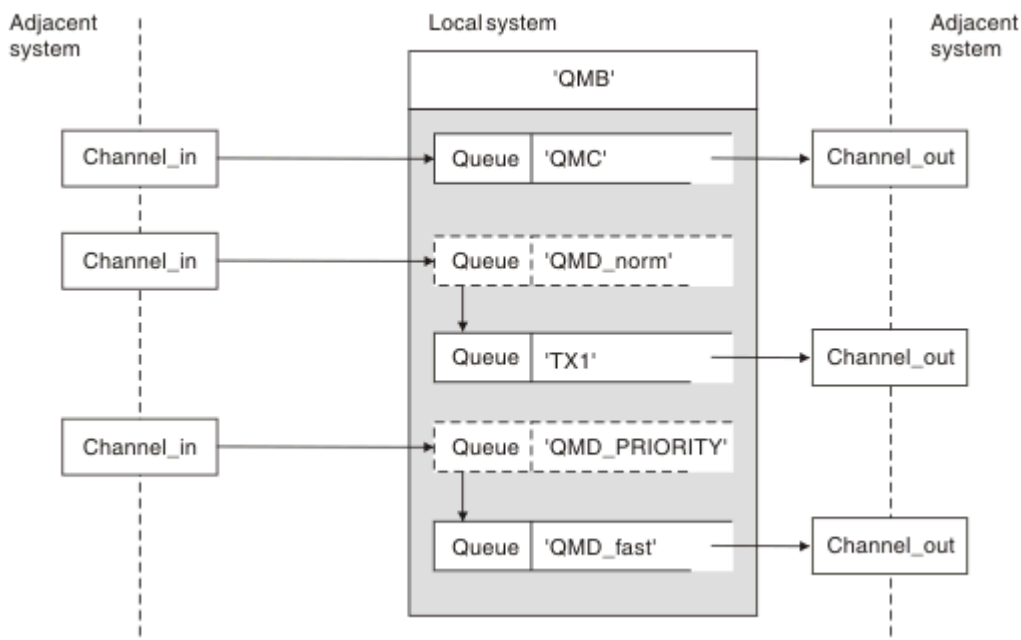
- Kanály zpráv pro příjem zpráv ze sousedních správců front
- Definice aliasu správce front k vyřešení příchozího toku zpráv, 'QMB_priority', do lokálního názvu správce front, 'QMB'
- Lokální fronta, 'QA_norm', pokud neexistuje,

Přijímání názvů správce front aliasu

Použití definice aliasu správce front v této ilustraci nevedlo k výběru jiného cílového správce front. Zprávy, které prošly tímto lokálním správcem front a adresované na 'QMB_priority', jsou určeny pro správce front 'QMB'. Název správce alias fronty se používá k vytvoření samostatného toku zpráv.

Předání zpráv prostřednictvím systému

Zprávy můžete předávat prostřednictvím systému třemi způsoby-pomocí názvu umístění, s použitím aliasu pro správce front nebo výběrem přenosové fronty.



Obrázek 9. Tři metody posílání zpráv přes váš systém

Technika zobrazená v [Obrázek 8 na stránce 129](#) v “Příjem zpráv” na stránce 129 ukázala, jak je zachycen tok alias. [Obrázek 9 na stránce 130](#) ilustruje, jak jsou sítě vybudovány tím, že dohromady techniky popsané dříve.

Konfigurace zobrazuje kanál doručující tři zprávy s různými místy určení:

1. QB rovno QMC
2. QB rovno QMD_norm
3. QB rovno QMD_PRIORITY

První tok zpráv musíte přenést prostřednictvím systému nezměněný. Druhý tok zpráv je třeba předat prostřednictvím jiné přenosové fronty a kanálu. Pro druhý tok zpráv je třeba také vyřešit zprávy pro název aliasu správce front QMD_noirm správci front QMD. Třetí tok zpráv zvolí jinou přenosovou frontu bez jakékoli jiné změny.

V klastrovém prostředí jsou zprávy předávány prostřednictvím přenosové fronty klastru. Za normálních okolností jedna přenosová fronta SYSTEM.CLUSTER.TRANSMIT.QUEUE přenáší všechny zprávy do všech správců front ve všech klastrech, jejichž členem je správce front; viz [Klastr správců front](#). Můžete definovat samostatné přenosové fronty pro všechny správce front nebo některé z nich v klastrech, jejichž členem je správce front.

Následující metody popisují metody použitelné pro prostředí s distribuovaným řazením do fronty.

Použit tyto metody

Pro tyto konfigurace musíte připravit:

- Definice vstupního kanálu
- Definice výstupního kanálu
- Přenosové fronty:
 - QMC
 - TX1
 - QMD_fast
- Definice aliasů správce front:
 - QMD_noirm with QMD_noirm to QMD through TX1
 - QMD_PRIORITY with QMD_PRIORITY to QMD_PRIORITY through QMD_fast

Poznámka: Žádná z toků zpráv zobrazených v příkladu nemění cílovou frontu. Alias názvu správce front poskytuje oddělení toků zpráv.

Metoda 1: Použit název příchozího umístění

Obdržíte zprávy s hlavičkou přenosu, která obsahuje jiné jméno umístění, jako např. QMC. Nejjednodušší konfigurací je vytvořit přenosovou frontu s tímto názvem, QMC. Kanál, který obsluhuje přenosovou frontu, předá zprávu nezměněnou na další místo určení.

Metoda 2: Použit alias pro správce front

Druhá metoda je použití definice alias objektu správce front, ale zadejte nový název umístění, QMDa konkrétní přenosovou frontu, TX1. Tato akce:

- Ukončí nastavení toku zpráv aliasů pomocí aliasu názvu správce front QMD_noirm, tj. pojmenované třídy služby QMD_noirm.
- Změní záhlaví přenosu na těchto zprávách z QMD_noirm na QMD.

Metoda 3: Vyberte přenosovou frontu

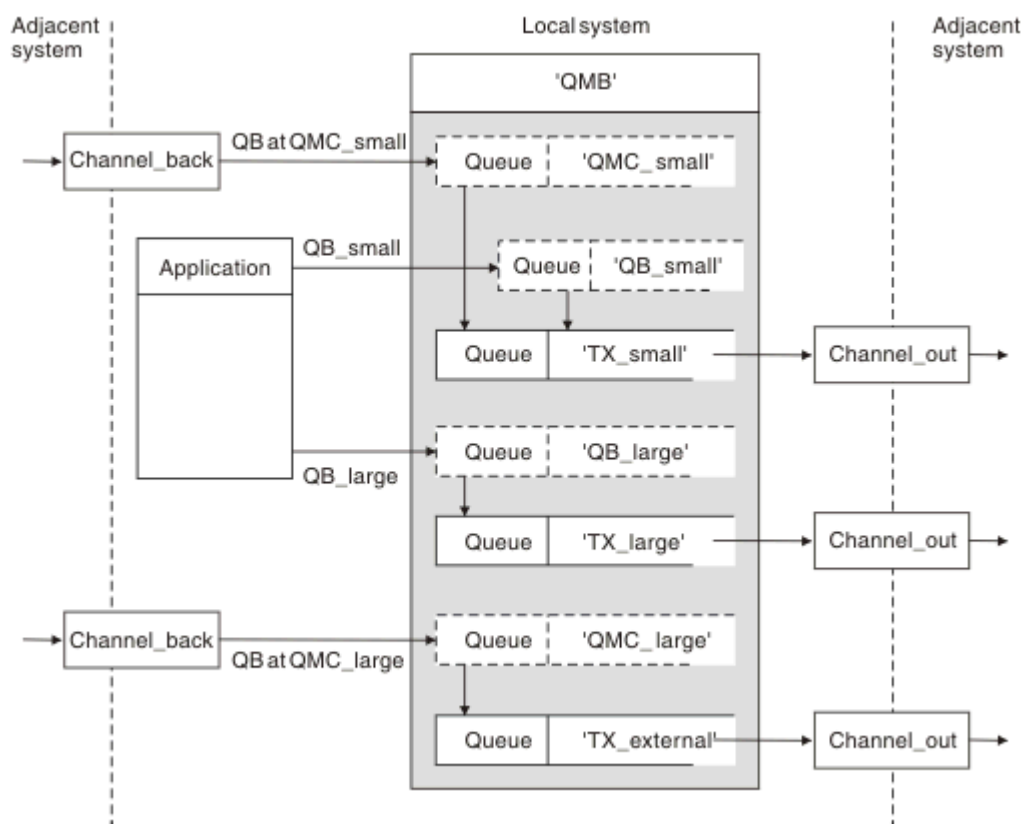
Třetí metodou je alias objektu správce front definovaný se stejným názvem jako cílové umístění, QMD_PRIORITY. Definice aliasu správce front slouží k výběru konkrétní přenosové fronty, produktu QMD_fast, a tedy jiného kanálu. Hlavičky přenosu na těchto zprávách zůstanou nezměněny.

Oddělování toků zpráv

Alias správce front můžete použít k vytvoření samostatných toků zpráv k odesílání zpráv do stejného správce front.

V prostředí s distribuovaným řazením může dojít k různým příčinám, že je třeba oddělit zprávy od stejného správce front do různých toků zpráv. Příklad:

- Je možné, že budete potřebovat samostatný tok pro velké, střední a malé zprávy. Tato potřeba se také používá v klastrovém prostředí, a v tomto případě můžete vytvářet klastry, které se překrývají. Existuje mnoho důvodů, proč byste tak mohli učinit, například:
 - Chcete-li umožnit různým organizacím, aby měly vlastní administraci.
 - Umožněte administraci nezávislých aplikací samostatně.
 - Vytvoření třídy služeb. Předpokládejme například, že máte klastr s názvem PERSONÁL, který je podmnožinou klastru s názvem STUDENTS. Když vložíte zprávu do fronty oznámené v klastru STAFF, bude použit vyhrazený kanál. Když vložíte zprávu do fronty oznámené v klastru STUDENTS, lze použít buď obecný kanál, nebo omezený kanál.
 - Vytvoření testovacího a produkčního prostředí.
- Je možné, že bude nutné směřovat příchozí zprávy různými cestami z cesty lokálně generovaných zpráv.
- Vaše instalace může vyžadovat naplánování přesunu zpráv v určitých časech (například přes noc) a zprávy pak musí být uloženy ve vyhrazených frontách, dokud není naplánováno.



Obrázek 10. Oddělení toků zpráv

V příkladu uvedeném v souboru Obrázek 10 na stránce 132 jsou dva příchozí toky alias názvů správce front 'QMC_small' a 'QMC_large'. Tyto toky jsou určeny pro zachycení těchto toků pro lokálního správce front pomocí definice alias správce front. Máte aplikaci adresující dvě vzdálené fronty a vy potřebujete tyto toky zpráv uchovávat odděleně. Poskytujete dvě definice vzdálených front, které určují stejné umístění, 'QMC', ale specifikujete různé přenosové fronty. Tato definice uchovává toky odděleně a v konečném důsledku není třeba nic dalšího, protože mají stejný cílový název správce front v záhlavích přenosu. Poskytujete:

- Definice příchozího kanálu
- Dvě definice vzdálených front QB_small a QB_large

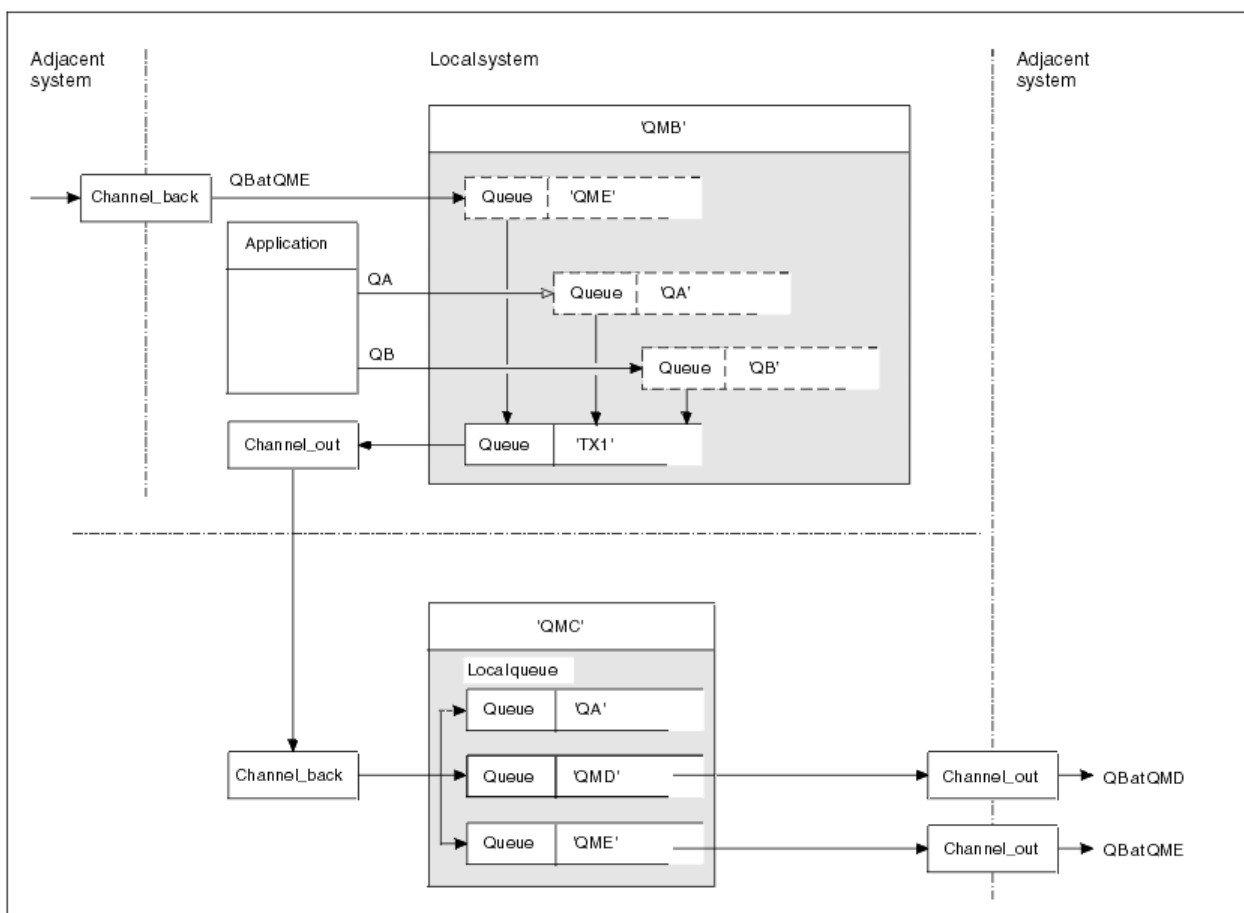
- Dva definice aliasů správce front QMC_small a QMC_large
- Tři definice odesílajícího kanálu
- Tři přenosové fronty: TX_small, TX_large, a TX_external

Koordinace se sousedními systémy

Používáte-li alias správce front k vytvoření samostatného toku zpráv, je třeba koordinovat tuto aktivitu s administrátorem systému na vzdáleném konci kanálu zpráv a zajistit tak, aby byl k dispozici odpovídající alias správce front.

Soustředění zpráv na různá místa

Můžete se soustředit na zprávy určené pro různá umístění na jednom kanálu.



Obrázek 11. Sloučení toků zpráv na kanál

Obrázek 11 na stránce 133 ilustruje techniku distribuované fronty pro soustředění zpráv, které jsou určeny pro různá umístění na jednom kanálu. Dvě možné použití by byla:

- Soustředí se na provoz zpráv prostřednictvím brány
- Použití širokých dálnic šířky pásma mezi uzly

V tomto příkladu jsou zprávy z různých zdrojů, lokální a sousední a mající různé cílové fronty a správce front odesílány prostřednictvím přenosové fronty 'TX1' ke správci front QMC správce front. Správce front QMC doručuje zprávy podle míst určených. Jedna sada do přenosové fronty 'QMD' pro další přenos do správce front QMD. Jiný je nastaven na přenosovou frontu 'QME' pro další přenos do správce front QME. Další zprávy jsou vloženy do lokální fronty 'QA'.

Musíte zadat:

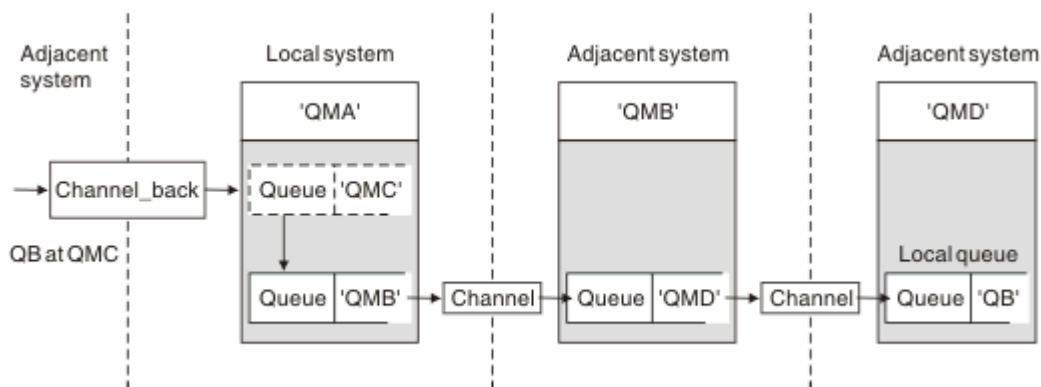
- Definice kanálů
- Přenosová fronta TX1
- Definice vzdálených front:
 - QA s QA v QMC přes TX1'
 - QB s 'QB při QMD přes TX1'
- Definice aliasu správce front:
 - QME se 'QME přes TX1'

Doplňkový administrátor, který konfiguruje QMC, musí poskytovat:

- Příjem definice kanálu se stejným názvem kanálu
- Přenosová fronta QMD s přidruženou definicí odesílajícího kanálu
- Přenosová fronta QME s přidruženou definicí odesílajícího kanálu
- Lokální objekt fronty QA.

Odklonění toku zpráv do jiného cíle

Můžete předefinovat místo určení určitých zpráv pomocí aliasů správce front a přenosových front.



Obrázek 12. Odklonění proudů zpráv do jiného cíle

Obrázek 12 na stránce 134 ilustruje, jak můžete předefinovat místo určení určitých zpráv. Příchozí zprávy pro QMA jsou určeny pro 'QB v QMC'. Běžně se dostanou do QMA a budou umístěny do přenosové fronty s názvem QMC, která byla součástí kanálu do QMC. QMA musí odklonit zprávy na QMD, ale je schopen dosáhnout pouze QMD přes QMB. Tato metoda je užitečná, když potřebujete přesunout službu z jednoho umístění do jiného a umožnit odběratelům pokračovat v odesílání zpráv dočasným způsobem, dokud se nepřizpůsobují nové adrese.

Metoda opětovného mapování příchozích zpráv určených pro určitého správce front do jiného správce front:

- Alias správce front pro změnu cílového správce front na jiného správce front a výběr přenosové fronty pro sousední systém.
- Přenosová fronta, která má sloužit sousednímu správci front
- Přenosová fronta v sousedním správci front pro následné směrování do cílového správce front.

Musíte zadat:

- Definice kanálu Channel_back
- Definice alias objektu správce front QMC s QB při QMD až QMB
- Definice objektu Channel_out
- Přidružená přenosová fronta QMB

Další administrátor, který konfiguruje QMB, musí poskytovat:

- Odpovídající definice channel_back
- Přenosová fronta, QMD
- Přidružená definice kanálu pro QMD.

Aliases lze používat v klastrovém prostředí. Informace viz [“Aliases správce front a klastry”](#) na stránce 306.

Odesílání zpráv do rozdělovníku

Chcete-li aplikaci odeslat zprávu do několika míst určení, můžete použít jediné volání MQPUT.

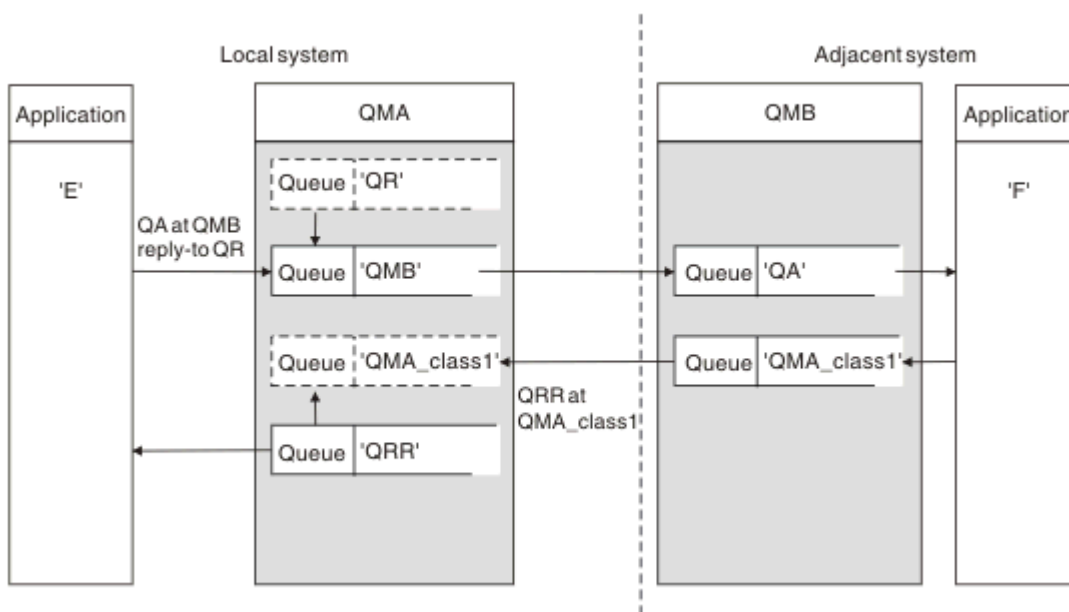
Ve IBM MQ na všech platformách kromě z/OS může aplikace odeslat zprávu do několika cílů s jedním voláním MQPUT. Můžete to provést jak v prostředí rozděleném do front, tak i v prostředí klastrů. Musíte definovat cíle v rozdělovníku, jak je popsáno v tématu [Distribuční seznamy](#).

Ne všichni správci front podporují distribuční seznamy. Když agent MCA naváže spojení s partnerem, určí, zda partner podporuje rozdělovníky a nastaví příznak přenosové fronty na odpovídajícím způsobem. Pokud se aplikace pokusí odeslat zprávu, která je určena pro distribuční seznam, ale partner nepodporuje distribuční seznamy, odesílající agent MCA zachytí zprávu a vloží ji do přenosové fronty jednou pro každé zamýšlené místo určení.

Přijímající agent MCA zajistí, aby zprávy odeslané do distribučního seznamu byly bezpečně přijaty ve všech zamýšlených cílech. Pokud některá místa určení selžou, agent MCA zjistí, které z nich selhaly. Pak může generovat zprávy o výjimkách pro ně a může se pokusit o jejich odeslání znovu.

Fronta pro odpověď

Můžete vytvořit úplnou smyčku zpracování vzdálených front pomocí fronty pro odpovědi.



Obrázek 13. Substituce názvu fronty pro odpověď během volání PUT

V produktu Obrázek 13 na stránce 135 se zobrazí úplná smyčka zpracování vzdálených front s použitím fronty pro odpověď. Tato smyčka se používá jak v prostředí s rozdělenou do front, tak i v prostředí klastrů. Podrobnosti jsou uvedeny v tématu [Tabulka 19](#) na stránce 142.

Aplikace otevře QA na QMB a vloží zprávy do této fronty. Pro zprávy je zadán název fronty QR pro odpověď bez správce front, který je určen. Správce front QMA nalezne objekt QR s odpovědí na frontu QR a extrahuje z něj alias QRR a název správce front QMA_class1. Tyto názvy jsou vloženy do polí pro odpověď na zprávy.

Odpovědi na zprávy z aplikací v QMB jsou adresovány na QRR na QMA_class1. Definice názvu aliasu správce front QMA_class1 je používána správcem front k toku zpráv do sebe sama a do fronty QRR.

Tento scénář popisuje způsob, jakým aplikacím poskytnete službu pro výběr třídy služeb pro zprávy odpovědi. Třída je implementována přenosovou frontou QMA_class1 v QMB, spolu s definicí aliasu správce front QMA_class1 na QMA. Tímto způsobem můžete změnit odpověď aplikace na frontu tak, aby toky byly odděleny, aniž by bylo třeba aplikace zahrnovat. Aplikace vždy volí QR pro tuto konkrétní třídu služeb. Máte možnost změnit provozní třídu s definicí QR odpovědi na frontu pro odpověď.

Musíte vytvořit:

- QR definice odpovědi na frontu
- QMB objektu přenosové fronty
- Definice objektu Channel_out
- Definice kanálu Channel_back
- Definice aliasu správce front QMA_class1
- Objekt lokální fronty QRR, pokud neexistuje

Další administrátor v sousedním systému musí vytvořit:

- Definice přijímajícího kanálu
- Objekt přenosové fronty QMA_class1
- Přidružený odesílající kanál
- Lokální objekt fronty QA.

Vaše aplikační programy používají:

- Název fronty pro odpověď na název fronty QR při vložení volání
- Název fronty QRR pro volání get

Tímto způsobem můžete podle potřeby změnit provozní třídu, aniž by bylo nutné aplikaci používat. Změňte odpověď na alias 'QR', spolu s přenosovou frontou 'QMA_class1' a aliasem správce front 'QMA_class1'.

Není-li při vložení zprávy do fronty nalezen žádný objekt aliasu pro odpověď na alias, bude název lokálního správce front vložen do prázdného pole názvu správce front pro odpověď. Název fronty pro odpovědi zůstává nezměněn.

Omezení rozlišování názvů

Vzhledem k tomu, že při vložení původní zprávy bylo provedeno rozpoznání názvu pro frontu pro odpověď na frontu 'QMA', není povoleno žádné další rozlišení názvu v 'QMB'. Zpráva se umístí s fyzickým názvem odpovědi do fronty odpovědí aplikací.

Aplikace si musí být vědomy toho, že název, který používají pro frontu pro odpověď, se liší od názvu skutečné fronty, kde se mají vratové zprávy nalézt.

Když jsou například pro použití aplikací s aliasy fronty pro odpověď na aliasC1_alias'a'C2_alias' poskytnuty dvě třídy služeb, používají aplikace tyto názvy jako názvy front pro odpověď ve volaných volaných zprávách. However, the applications actually expect messages to appear in queues 'C1' for 'C1_alias' and 'C2' for 'C2_alias'.

Avšak aplikace je schopna provést dotazové volání na frontu alias pro odpověď, aby zkontroloval jméno skutečné fronty, kterou musí použít k získání zpráv odpovědi.

Související pojmy

[“Jak vytvořit správce front a odpovědět na aliasy” na stránce 126](#)

Toto téma vysvětluje tři způsoby, jak můžete vytvořit definici vzdálené fronty.

[“Příklad alias fronty pro odpověď” na stránce 137](#)

Tento příklad ilustruje použití aliasu odpovědi na alias pro výběr jiné přenosové cesty (přenosové fronty) pro vrácené zprávy. Použití této funkce vyžaduje, aby se název fronty pro odpověď změnil ve spolupráci s aplikacemi.

“Jak příklad funguje” na stránce 138

Vysvětlení příkladu a způsobu, jakým správce front používá alias fronty pro odpověď.

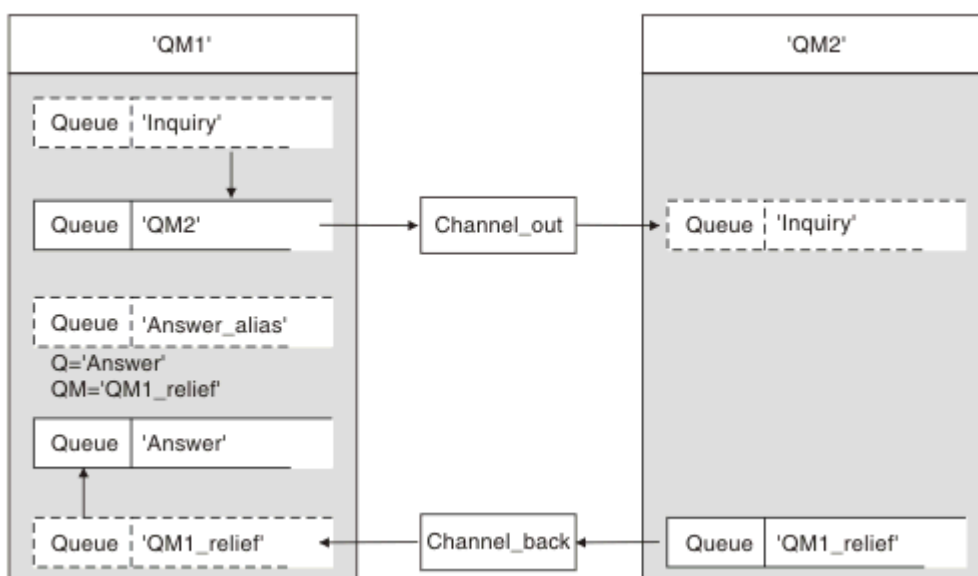
“Průchodná odpověď na alias fronty pro odpověď” na stránce 139

Průchod procesu z aplikace, který vkládá zprávu do vzdálené fronty do stejné aplikace a odebírá zprávu odpovědi z alias odpovědi alias.

Příklad alias fronty pro odpověď

Tento příklad ilustruje použití aliasu odpovědi na alias pro výběr jiné přenosové cesty (přenosové fronty) pro vrácené zprávy. Použití této funkce vyžaduje, aby se název fronty pro odpověď změnil ve spolupráci s aplikacemi.

Jak je zobrazeno v Obrázek 14 na stránce 137, zpáteční cesta musí být k dispozici pro zprávy odpovědi včetně alias přenosové fronty, kanálu a aliasu správce front.



Obrázek 14. Příklad alias fronty pro odpověď

Tento příklad je určen pro aplikace žadatele na 'QM1', které posílají zprávy do aplikací serveru na 'QM2'. Zprávy na serveru se mají vracet prostřednictvím alternativního kanálu s použitím přenosové fronty 'QM1_relief' (výchozí návratový kanál bude obsluhován s přenosovou frontou 'QM1').

Alias fronty pro odpověď je konkrétní použití definice vzdálené fronty s názvem 'Answer alias'. Aplikace v QM1 zahrnují tento název, 'Answer_alias', v poli odpovědi na všechny zprávy, které vložili do fronty 'Inquiry'.

Definice fronty odpovědi 'Answer alias' je definována jako 'Answer at QM1_relief'. Aplikace v QM1 očekávají, že se jejich odpovědi zobrazí v lokální frontě s názvem 'Answer'.

Serverové aplikace na úrovni QM2 používají pole odpovědi na přijaté zprávy k získání názvů front a správců front pro zprávy odpovědi žadateli na QM1.

Definice použité v tomto příkladu na QM1

Administrátor systému IBM MQ na QM1 musí zajistit, aby byla vytvořena odpověď na frontu 'Answer' spolu s dalšími objekty. Název aliasu správce front označený pomocí znaku '*' musí souhlasit s názvem správce front v definici alias fronty pro odpověď, který je také označen jako '*'.

Objekt	Definice	
Lokální přenosová fronta	QM2	
Definice vzdálené fronty	Název objektu	Inquiry
	Název vzdáleného správce front	QM2
	Název vzdálené fronty	Inquiry
	Jméno přenosové fronty	QM2 (DEFAULT)
Alias správce front	Název objektu	QM1_relief *
	Název správce front	QM1
	Název fronty	(prázdné)
Alias fronty pro odpověď	Název objektu	alias_odpovědi
	Název vzdáleného správce front	QM1_relief *
	Název vzdálené fronty	Přijmout

Definice vložení na QM1

Aplikace vyplňují odpověď na pole s názvem aliasu fronty odpovědí a ponechte pole názvu správce front prázdné.

Pole	Obsah
Název fronty	Inquiry
Název správce front	(prázdné)
Název fronty pro odpověď	alias_odpovědi
Správce front pro odpovědi	(prázdné)

Definice použité v tomto příkladu na QM2

Administrátor systému IBM MQ na QM2 se musí ujistit, že lokální fronta existuje pro příchozí zprávy a že správně pojmenovaná přenosová fronta je k dispozici pro zprávy odpovědi.

Objekt	Definice
Lokální fronta	Inquiry
Přenosová fronta	QM1_relief

Definice vložení na QM2

Aplikace v QM2 načtou název fronty a název správce front z původní zprávy a použijí je při vložení zprávy odpovědi do fronty pro odpověď.

Pole	Obsah
Název fronty	Přijmout
Název správce front	QM1_relief

Jak příklad funguje

Vysvětlení příkladu a způsobu, jakým správce front používá alias fronty pro odpověď.

V tomto příkladu aplikace žadatele v QM1 vždy používají 'Answer alias' jako frontu pro odpověď v příslušném poli volání příkazu put. Vždy načtou své zprávy z fronty s názvem 'Odpověď'.

Definice alias fronty pro odpověď jsou k dispozici pro použití administrátorem systému QM1 ke změně názvu odpovědi na frontu odpovědi a návratové cesty 'QM1_relief'.

Změna názvu fronty 'Answer' je obvykle neúčinná, protože aplikace QM1 očekávají své odpovědi v této frontě. Administrátor systému QM1 však může podle potřeby změnit návratovou trasu (třídou služeb).

Jak správce front používá alias fronty odpovědi na frontu

Správce front QM1 načte definice z aliasu fronty pro odpověď, je-li název fronty pro odpověď, zahrnutý v volaném volání aplikace, stejný jako alias fronty pro odpověď a část správce front je prázdná.

Správce front nahradí název fronty pro odpověď v umístění volání s názvem fronty z definice. Nahrazuje prázdný název správce front v rámci volání put s názvem správce front z definice.

Tyto názvy jsou přenášeny spolu se zprávou v deskriptoru zpráv.

<i>Tabulka 16. Alias fronty pro odpověď</i>		
Název pole	Volání vložení	Hlavička přenosu
Název fronty pro odpověď	alias_odpovědi	Přijmout
Název správce front pro odpověď	(prázdné)	QM1_relief

Průchodná odpověď na alias fronty pro odpověď

Průchod procesu z aplikace, který vkládá zprávu do vzdálené fronty do stejné aplikace a odebírá zprávu odpovědi z alias odpovědi alias.

Chcete-li dokončit tento příklad, podívejme se na proces.

1. Aplikace otevře frontu s názvem 'Inquiry' a vloží do ní zprávy. Aplikace nastaví pole odpovědi na pole deskriptoru zprávy na:

Název fronty pro odpověď	alias_odpovědi
Název správce front pro odpověď	(prázdné)

2. Správce front 'QM1' odpovídá na prázdný název správce front tím, že zkontroluje definici vzdálené fronty s názvem 'Answer alias'. Není-li nalezena žádná hodnota, správce front umístí své vlastní jméno 'QM1' do pole správce front pro odpověď na deskriptor zprávy.
3. Pokud správce front nalezne definici vzdálené fronty s názvem 'Answer alias', extrahuje název fronty a názvy správce front z definice (název fronty= 'Answer' a správce front name= 'QM1_relief'). Pak je umístí do polí deskriptoru zpráv do odpovědi.
4. Správce front 'QM1' používá definici vzdálené fronty 'Inquiry', aby určil, že zamýšlená cílová fronta je ve správci front 'QM2', a zpráva se umístí do přenosové fronty 'QM2'. 'QM2' je výchozí název přenosové fronty pro zprávy určené pro fronty ve správci front 'QM2'.
5. Když správce front 'QM1' vloží zprávu do přenosové fronty, přidá do zprávy záhlaví přenosu. Toto záhlaví obsahuje název cílové fronty, 'Inquiry' a správce cílové fronty 'QM2'.
6. Zpráva dorazí do správce front 'QM2' a je umístěna v lokální frontě 'Inquiry'.
7. Aplikace získá zprávu z této fronty a zpracuje zprávu. Aplikace připraví zprávu odpovědi a vloží tuto zprávu odpovědi na název fronty pro odpovědi z deskriptoru zprávy původní zprávy:

Název fronty pro odpověď	Přijmout
Název správce front pro odpověď	QM1_relief

8. Správce front 'QM2' provádí příkaz put. Nalezení názvu správce front QM1_relief je vzdáleným správcem front, který umístí zprávu do přenosové fronty se stejným názvem, 'QM1_relief'. Zobrazí se zpráva obsahující záhlaví přenosu obsahující název cílové fronty, 'Odpověď' a správce cílové fronty 'QM1_relief'.
9. Zpráva se přenesou do správce front 'QM1'. Správce front rozpozná, že název správce front 'QM1_relief' je alias, extrakty z definice aliasu 'QM1_relief', název správce fyzických front 'QM1'.

10. Správce front 'QM1' pak vloží zprávu do názvu fronty obsaženého v záhlaví přenosu, 'Answer'.

11. Aplikace extrahuje svou zprávu odpovědi z fronty 'Answer'.

Faktory související


V prostředí s distribuovaným řazením do fronty, protože cíle zpráv jsou adresovány pouze s názvem fronty a názvem správce front, platí určitá pravidla.

1. Je-li zadán název správce front a název se liší od názvu lokálního správce front, postupujte takto:

- Přenosová fronta musí být k dispozici se stejným názvem. Tato přenosová fronta musí být součástí kanálu zpráv přesouváním zpráv do jiného správce front, nebo
- Definice aliasu správce front musí existovat, aby bylo možné název správce front převést na stejný nebo jiný název správce front a volitelnou přenosovou frontu, nebo
- Pokud nemůže být název přenosové fronty vyřešen a byla definována výchozí přenosová fronta, použije se výchozí přenosová fronta.

2. Je-li zadán pouze název fronty, musí být ve správci lokální fronty k dispozici fronta libovolného typu, ale se stejným názvem. Tato fronta může být definicí vzdálené fronty, která se řeší jako: přenosová fronta se sousedním správcem front, názvem správce front a volitelnou přenosovou frontou.

Informace o tom, jak to funguje v klastrovém prostředí, najdete v tématu [Klustry](#).

 Jsou-li správci front spuštěni ve skupině sdílení front (QSG) a ve frontě v rámci skupiny (IGQ) je povoleno, můžete použít SYSTEM.QSG.TRANSMIT.QUEUE. Další informace naleznete v tématu [Řazení do front v rámci skupiny](#).

Zvažte scénář přesunu zpráv kanálu zpráv z jednoho správce front do jiného v prostředí s distribuovaným řazením do fronty.

Přesunuté zprávy pocházely z libovolného jiného správce front v síti a některé zprávy mohou přicházet s neznámým názvem správce front jako cíl. K tomuto problému může dojít, když se název správce front například změnil nebo byl odebrán ze systému.

Program kanálu rozpozná tuto situaci, když nemůže najít přenosovou frontu pro tyto zprávy, a umístí zprávy do fronty nedoručených zpráv (dead-letter). Je vaší zodpovědností hledat tyto zprávy a zařídit, aby byly přesměrovány na správné místo určení. Případně je vraťte původci, kde je možné původce zjistit.

Za těchto okolností jsou generovány zprávy o výjimkách, pokud byly zprávy sestavy požadovány v původní zprávě.

Konvence rozpoznávání názvů

Rozpoznání názvu, které mění identitu cílové fronty (tj. se změnou fyzického názvu), se vyskytuje pouze jednou a pouze u původního správce front.

Následné použití různých možností aliasu musí být použito pouze při oddělování a kombinování toků zpráv.

Zpětné směřování

Zprávy mohou obsahovat návratovou adresu ve formě názvu fronty a správce front. Tento formulář návratové adresy lze použít jak v prostředí s rozdělenou do front, tak i v prostředí klastrů.

Tato adresa je obvykle určena aplikací, která vytváří zprávu. Může být upraven libovolnou aplikací, která pak tuto zprávu zpracovává, včetně aplikací uživatelské procedury.

Bez ohledu na zdroj této adresy může každá aplikace zpracovávající zprávu zvolit použití této adresy pro vrácení odpovědi, stavu nebo zprávy hlášení do původní aplikace.

Způsob, jakým jsou tyto zprávy odezvy směřovány, se liší od způsobu, jakým je směřována původní zpráva. Musíte si být vědomi toho, že toky zpráv, které vytvoříte k jiným správcům front, potřebují odpovídající návratové toky.

Konflikty fyzických názvů

Název cílové hodnoty fronty pro odpověď byl vyřešen na název fyzické fronty v původním správci front. Nesmí být znovu rozlišena u odpovídajícího správce front.

Je pravděpodobné, že se mohou vyskytnout problémy s konfliktem názvů, které může být bráněno pouze sítí v rámci sítě ve fyzických a logických názvech front.

Správa překladů názvů front

Při vytváření definice aliasu správce front nebo definice vzdálených front je pro každou zprávu, která tento název obsahuje, provedeno rozpoznávání názvů. Tato situace musí být spravována.

Tento popis je určen pro návrháře aplikací a plánovače kanálů, které se zabývají jednotlivým systémem, který má kanály zpráv pro sousední systémy. Zabere to místní pohled na plánování a řízení kanálů.

Při vytváření definice aliasu správce front nebo definice vzdálených front je pro každou zprávu, která tento název obsahuje, prováděno rozpoznávání názvů bez ohledu na zdroj této zprávy. Chcete-li dohlédnout na tuto situaci, která může zahrnovat velký počet front v síti správce front, zachovávají si následující tabulky:

- Názvy zdrojových front a správců zdrojových front s ohledem na vyřešené názvy front, vyřešených názvů správců front a rozlišených názvů přenosových front s použitím metody rozpoznání
- Názvy zdrojových front s ohledem na:
 - Vyřešené názvy cílových front
 - Vyřešené názvy správce cílových front
 - Přenosové fronty
 - Názvy kanálů zpráv
 - Jména sousedního systému
 - Názvy front pro odpověď

Poznámka: Použití výrazu *source* v tomto kontextu se vztahuje k názvu fronty nebo názvu správce front poskytovaného aplikací nebo programu kanálu při otevírání fronty pro vkládání zpráv.

Příklad každé z těchto tabulek je zobrazen v [Tabulka 17 na stránce 141](#), [Tabulka 18 na stránce 142a](#) [Tabulka 19 na stránce 142](#).

Názvy v těchto tabulkách jsou odvozeny z příkladů uvedených v tomto oddíle a tato tabulka není zamýšlena jako praktický příklad rozlišení názvů front v jednom uzlu.

Zdrojová fronta uvedená při otevření fronty	Zdrojový správce front uvedený při otevření fronty	Rozlišený název fronty	Vyřešený název správce front	Vyřešený název přenosové fronty	Typ rozlišení
QA_norm	-	QA_norm	QMB	QMB	Vzdálená fronta
(libovolný)	QMB	-	-	QMB	(není)
QA_norm	-	QA_norm	QMB	TX1	Vzdálená fronta
QB	QMC	QB	QMD	QMB	Alias správce front

Zdrojová fronta uvedená při otevření fronty	Zdrojový správce front uvedený při otevření fronty	Rozlišený název fronty	Vyřešený název správce front	Vyřešený název přenosové fronty	Typ rozlišení
QA_norm	-	QA_norm	QMB	-	(není)
QA_norm	QMB	QA_norm	QMB	-	(není)
QA_norm	PRIORITA QMB_PRIORITY	QA_norm	QMB	-	Alias správce front
(libovolný)	QMC	(libovolný)	QMC	QMC	(není)
(libovolný)	QMD_norm	(libovolný)	QMD_norm	TX1	Alias správce front
(libovolný)	PRIORITA QMD_PRIORITY	(libovolný)	PRIORITA QMD_PRIORITY	QMD_fast	Alias správce front
(libovolný)	QMC_small	(libovolný)	QMC_small	TX_small	Alias správce front
(libovolný)	QMC_large	(libovolný)	QMC_large	TX_externí	Alias správce front
QB_small	QMC	QB_small	QMC	TX_small	Vzdálená fronta
QB_large	QMC	QB_large	QMC	TX_large	Vzdálená fronta
(libovolný)	QME	(libovolný)	QME	TX1	Alias správce front
QA	QMC	QA	QMC	TX1	Vzdálená fronta
QB	QMD	QB	QMD	TX1	Vzdálená fronta

Návrh aplikací		Definice aliasu pro odpověď	
Lokální správce front	Název fronty pro zprávy	Název aliasu fronty pro odpověď	Redefinováno na
QMA	QRR	OR.	QRR na QMA_class1

Pořadové číslování zpráv kanálu

Kanál používá pořadová čísla, aby zkontroloval, že zprávy jsou doručeny ve stejném pořadí, v jakém byly převzaty z přenosové fronty.

Číslo posloupností kanálů se kontrolují při spuštění kanálu a dojde k neshodě, znamená to, že trvalá data synchronizace byla ztracena na obou stranách kanálu; například konfigurace zotavení z havárie (DR) nebo ukončení dávkového zpracování byla přerušena, když byl kanál v nejistém stavu.

Zadání příkazu RESET CHANNEL nezpůsobí ztrátu nebo duplikaci zpráv. RESET potvrdí varování z IBM MQ, že se něco nezdá být správné. Neověřený kanál, který ztratil trvalý stav, se stále nedaří spustit po RESETu, dokud nevydáte příkaz RESOLVE CHANNEL; je to akce, která má potenciál ke ztrátě nebo duplikaci dávky.

Tyto informace lze zobrazit pomocí příkazu DISPLAY CHSTATUS. Pořadové číslo a identifikátor nazývaný LUWID jsou uloženy v trvalém úložišti pro poslední zprávu přenesenou v dávce. Tyto hodnoty se používají během spuštění kanálu, aby se zajistilo, že oba konce vazby souhlasí s tím, že zprávy byly úspěšně přeneseny.

Sekvenční načítání zpráv

Pokud aplikace vkládá posloupnost zpráv do stejné cílové fronty, tyto zprávy mohou být načteny v posloupnosti pomocí aplikace **jedna** s posloupností operací MQGET, jsou-li splněny následující podmínky:

- Všechny požadavky na vložení byly provedeny ze stejné aplikace.
- Všechny požadavky na vložení byly buď ze stejné pracovní jednotky, nebo všechny požadavky na vložení byly provedeny mimo jednotku práce.
- Všechny zprávy mají stejnou prioritu.
- Všechny zprávy mají stejnou perzistenci.
- Pro vzdálené fronty je konfigurace taková, že může existovat pouze jedna cesta z aplikace provádějící požadavek na vložení přes správce front, přes interkomunikaci, do cílového správce front a do cílové fronty.
- Zprávy se nevloží do fronty nedoručených zpráv (například, je-li fronta dočasně plná).
- Aplikace, která získává zprávu, neúmyslně mění pořadí načítání, například zadáním konkrétního *MsgId* nebo *CorrelId* nebo použitím priorit zpráv.
- Pouze jedna aplikace provádí operace načtení pro načtení zpráv z cílové fronty. Pokud existuje více než jedna aplikace, tyto aplikace musí být navrženy tak, aby všechny zprávy byly získány v každé posloupnosti odeslané odesílající aplikací.

Poznámka: Zprávy z jiných úloh a jednotek práce mohou být provázané s posloupností, a to i tam, kde byla posloupnost vložena v rámci jedné pracovní jednotky.

Pokud tyto podmínky nemohou být splněny a pořadí zpráv na cílové frontě je důležité, pak lze aplikaci naprogramovat, aby používala vlastní pořadové číslo zprávy jako část zprávy, aby se zajistilo pořadí zpráv.

Posloupnost načítání rychlých přechodných zpráv

Přechodné zprávy v rychlém kanálu mohou přepsat trvalé zprávy na stejném kanálu a tak se dostaví mimo pořadí. Přijímající agent MCA okamžitě umístí přechodné zprávy do cílové fronty a zviditelní je. Trvalé zprávy nejsou viditelné až do dalšího bodu synchronizace.

Testování zpětné smyčky

Testování zpětné smyčky je technika na jiných platformách než z/OS, která umožňuje testovat komunikační spojení bez skutečného propojení s jiným počítačem.

Nastavili jste spojení mezi dvěma správci front, jako kdyby byli na samostatných počítačích, ale otestovali jste připojení pomocí cyklu na jiném procesu na stejném počítači. Tato technika znamená, že můžete testovat svůj komunikační kód, aniž byste museli vyžadovat aktivní síť.

Způsob, jakým to uděláte, závisí na tom, které produkty a protokoly používáte.

V systému Windows můžete použít adaptér "loopback".

Další informace naleznete v dokumentaci k produktům, které používáte.

Trasování přenosové cesty a záznam aktivity

Můžete potvrdit trasu, kterou zpráva prochází řadou správců front dvěma způsoby.

Můžete použít aplikaci trasy zobrazení IBM MQ, která je k dispozici prostřednictvím řídicího příkazu `dspmqrte`, nebo můžete použít záznam aktivity. Obě tato témata jsou popsána v tématu [Odkaz na monitorování](#).

Úvod do distribuované správy front

Distribuovaná správa front (DQM) se používá k definování a řízení komunikace mezi správci front.

Správa distribuovaných front:




- Umožňuje vám definovat a řídit komunikační kanály mezi správci front.
- Poskytuje vám službu kanálu zpráv k přesouvání zpráv z typu *lokální fronty*, známého jako přenosová fronta, do komunikačních linek na lokálním systému a z komunikačních spojení do lokálních front v cílovém správci front.
- Poskytuje nástroje pro monitorování činnosti kanálů a diagnostiku problémů, použití panelů, příkazů a programů.

Definice kanálů přidružují názvy kanálů k přenosovým frontám, identifikátorům komunikačního propojení a atributům kanálů. Definice kanálů jsou implementovány různými způsoby na různých platformách. Odesílání a příjem zpráv je řízeno programy známými jako *agenti kanálu zpráv* (MCA), které používají definice kanálu k zahájení a řízení komunikace.





Kontrolované MCoby jsou řízeny samotným řízením kvality dat. Struktura je závislá na platformě, ale zpravidla obsahuje listenery a monitory spouštěčů, spolu s příkazy a panely operátora.

Kanál zpráv je jednosměrné propojení procesů pro přesouvání zpráv z jednoho správce front do jiného. Takže kanál zpráv má dva koncové body, představované dvojicí jednotek MCA. Každý koncový bod má definici svého konce kanálu zpráv. Jeden konec by například definoval odesílatele, druhý konec příjemce.

Podrobnosti o tom, jak definovat kanály, najdete v tématu:

-  [“Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux” na stránce 173](#)
-  [“Monitorování a řízení kanálů v systému z/OS” na stránce 594](#)
-  [“Monitorování a řízení kanálů v systému IBM i” na stránce 195](#)

Příklady plánování kanálů zpráv viz:

-  [Příklad plánování kanálů zpráv pro distribuované platformy](#)
-  [Příklad plánování kanálů zpráv pro produkt IBM MQ for IBM i](#)
-  [Příklad plánování kanálů zpráv pro produkt z/OS](#)
-  [Příklad plánování kanálů zpráv pro produkt z/OS s použitím skupin sdílení front](#)

Informace o uživatelských procedurách kanálů naleznete v tématu [Programy výstupních programů kanálů pro kanály systému zpráv](#).

Související pojmy

[“Odeslání a příjem zprávy” na stránce 145](#)

Následující obrázek ukazuje model distribuované správy front s podrobnými informacemi o vztazích mezi entitami při přenosu zpráv. Zobrazuje také tok pro řízení.

[“Řídící funkce kanálu” na stránce 152](#)

Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

[“Co se stane, když nebude možné zprávu doručit?” na stránce 165](#)

Nelze-li zprávu doručit, může ji agent MCA zpracovat několika způsoby. Může to zkusit znovu, může vrátit odesílateli, nebo to může dát do fronty nedoručených zpráv.

[“Inicializační a konfigurační soubory” na stránce 169](#)

Způsob zpracování inicializačních dat kanálu závisí na platformě IBM MQ .

[“Převod dat” na stránce 171](#)

Zprávy produktu IBM MQ mohou vyžadovat převod dat při odesílání mezi frontami v různých správcích front.

[“Psaní vlastních agentů kanálů zpráv” na stránce 171](#)

IBM MQ vám umožňuje zapsat si vlastní programy MCA (Message Channel Agent) nebo instalovat jeden z nezávislých dodavatelů softwaru.

[“Další informace, které je třeba zvážit při správě distribuovaných front” na stránce 172](#)

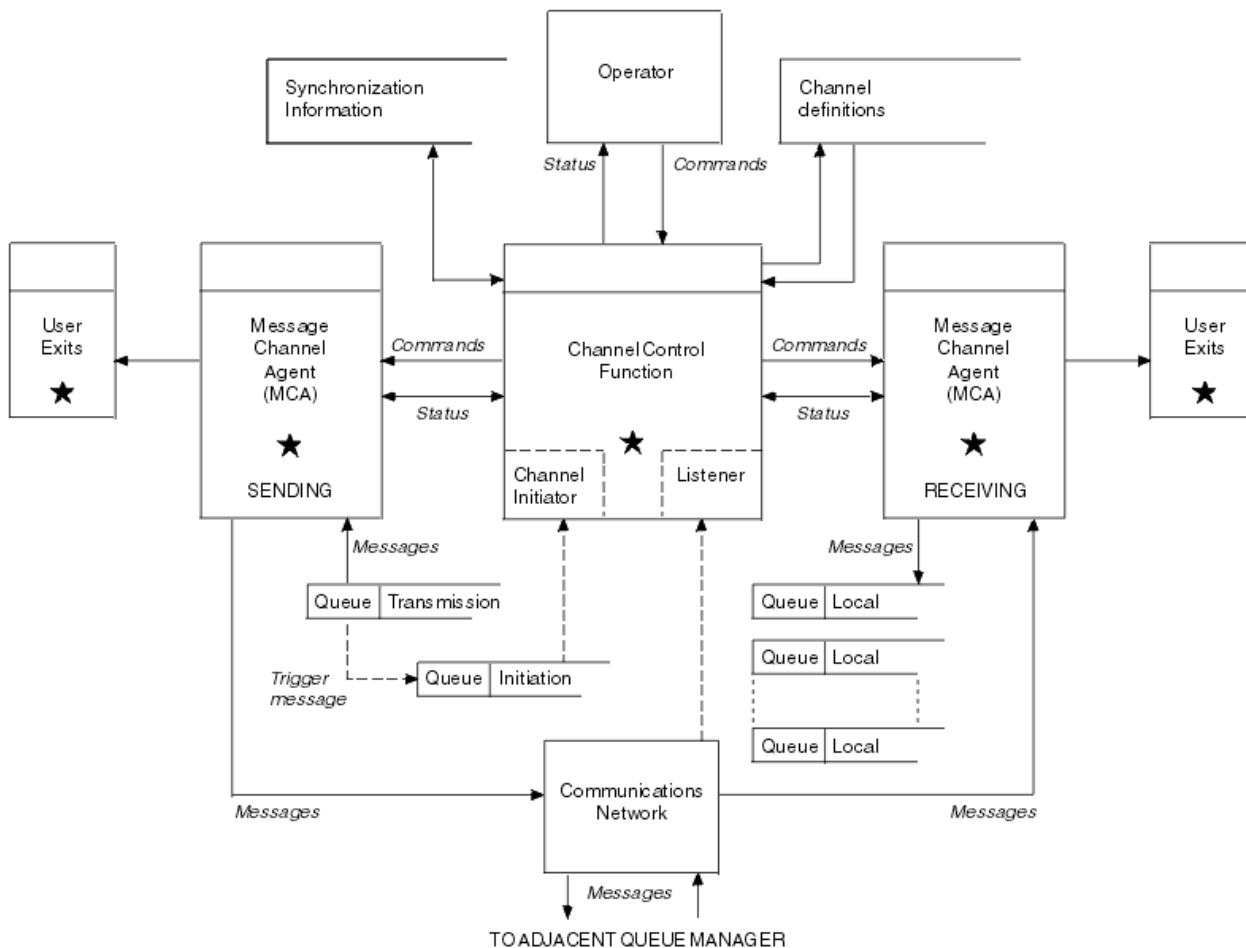
Další témata, která je třeba zvážit při přípravě produktu IBM MQ pro distribuovanou správu front. Toto téma pokrývá frontu nedoručených zpráv, Fronty v použití, Rozšíření systému a programy uživatelských procedur a Spouštění kanálů a listenerů jako ověřené aplikace.

Související informace

[Příklad konfiguračních informací](#)

Odeslání a příjem zprávy

Následující obrázek ukazuje model distribuované správy front s podrobnými informacemi o vztazích mezi entitami při přenosu zpráv. Zobrazuje také tok pro řízení.



Obrázek 15. Model distribuované správy front

Poznámka:

1. V závislosti na platformě je v závislosti na platformě jedna sběrnice MCA pro kanál. Pro určitého správce front může existovat jedna nebo více řídicích funkcí kanálu.
2. Implementace funkcí MCA a řídicích funkcí kanálu je závislá na platformě. Mohou být programy nebo procesy či podprocesy a mohou se jednat o jednu entitu nebo řadu z nich skládající se z několika nezávislých nebo propojených částí.
3. Všechny komponenty označené hvězdičkou mohou používat rozhraní MQI.

Parametry kanálu

MCA přijímá své parametry jedním z několika způsobů:

- Pokud je příkaz spuštěn příkazem, je v datové oblasti předán název kanálu. Agent MCA poté přečte definici kanálu přímo, aby získal její atributy.

- Pro odesílatele a v některých případech může být agent MCA spuštěn automaticky pomocí spouštěče správce front. Název kanálu je načten z definice procesu spouštěče, je-li to možné, a je předán do agenta MCA. Zbývající zpracování je stejné, jak bylo popsáno dříve. Kanály serveru musí být nastaveny pouze tak, aby se spouštěly, pokud jsou plně kvalifikované, to znamená, že určují hodnotu CONNAME, ke kterému se má připojit.
- Pokud je spuštěno vzdáleně odesílatelem, serverem, klientem nebo připojením klienta, předá se název kanálu v počátečních datech z partnerského agenta kanálu zpráv. Sběrnice MCA čte definici kanálu přímo za účelem získání jeho atributů.

Některé atributy, které nejsou definovány v definici kanálu, jsou také obchodovatelné:

Rozdělit zprávy

Pokud jeden konec nepodporuje rozdělené zprávy, pak se neodesílají rozdělené zprávy.

Schopnost převodu

Pokud jeden konec nemůže provést potřebnou konverzi kódové stránky nebo převod numerického kódování, je-li to nutné, druhý konec jej musí zpracovat. Pokud jej ani koncový bod nepodporuje, kanál nelze spustit.

Podpora seznamu distribuce

Pokud jeden konec nepodporuje distribuční seznamy, partnerský agent MCA nastaví příznak ve své přenosové frontě tak, že bude vědět, že zachytává zprávy určené pro více míst určení.

Stav kanálů a pořadová čísla

Programy agenta kanálu zpráv uchovávají záznamy o aktuálním pořadovém čísle a logické jednotce práce pro každý kanál a o obecném stavu kanálu. Některé platformy vám umožňují zobrazit tyto informace o stavu, které vám pomohou při řízení kanálů.

Jak odeslat zprávu jinému správci front


Tato sekce popisuje nejjednodušší způsob odeslání zprávy mezi správci front, včetně nezbytných předpokladů a požadovaných oprávnění. Další metody lze také použít k odeslání zpráv vzdálenému správci front.

Před odesláním zprávy z jednoho správce front do jiného je třeba provést následující kroky:



1. Zkontrolujte, zda je váš zvolený komunikační protokol k dispozici.
2. Spusťte správce front.
3. Spusťte iniciátory kanálu.
4. Spusťte listenery.

Musíte také mít správnou autorizaci zabezpečení produktu IBM MQ , abyste mohli vytvořit požadované objekty.

Chcete-li odeslat zprávy z jednoho správce front do jiného, postupujte takto:

- Definujte následující objekty ve zdrojovém správci front:
 - Kanál odesílatele
 - Definice vzdálené fronty
 - Inicializační fronta ( povinná na z/OS, jinak volitelné)
 - Přenosová fronta
 - Fronta nedoručených zpráv
- Definujte následující objekty v cílovém správci front:
 - Kanál příjemce
 - Cílová fronta
 - Fronta nedoručených zpráv

K definování těchto objektů můžete použít několik různých metod, v závislosti na vaší platformě IBM MQ :

- Na všech platformách můžete použít příkazy skriptů IBM MQ (MQSC) popsané v Příkazy MQSC programu pro programovatelné příkazy (PCF) popsané v příručce Automatizace administračních úloh nebo v Průzkumníku IBM MQ .
-  V systému z/OS můžete také použít panely Operace a Ovládací panely popsané v části Administrace produktu IBM MQ for z/OS .
-  V systému IBM i můžete také použít rozhraní panelu.

Další informace o vytváření komponent pro odesílání zpráv do jiného správce front naleznete v následujících dílčích tématech:

Související pojmy

“Vytváření a údržba správců front na distribuovaných platformách” na stránce 5

Než budete moci používat zprávy a fronty, musíte vytvořit a spustit alespoň jednoho správce front a jeho přidružené objekty.

“IBM MQ technologie distribuovaných front” na stránce 124

Dílčí témata v tomto oddílu popisují techniky, které se používají při plánování kanálů. Tato dílčí témata popisují techniky, které vám pomohou naplánovat vzájemné propojení správců front a správu toku zpráv mezi vašimi aplikacemi.

“Úvod do distribuované správy front” na stránce 143

Distribuovaná správa front (DQM) se používá k definování a řízení komunikace mezi správci front.

“Spouštěcí kanály” na stránce 166

Produkt IBM MQ poskytuje službu pro automatické spouštění aplikace, jsou-li splněny určité podmínky ve frontě. Toto zařízení se nazývá spouštění.

“Bezpečnost zpráv” na stránce 164

Kromě typických funkcí zotavení produktu IBM MQ zajišťuje distribuovaná správa front, že zprávy jsou řádně doručovány pomocí procedury synchronizačního bodu koordinované mezi dvěma konci kanálu zpráv. Pokud tento postup zjistí chybu, zavře kanál tak, abyste mohli problém vyšetřit a bezpečně uchovávat zprávy v přenosové frontě, dokud nebude kanál restartován.

“Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux” na stránce 173

Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, aplikací IBM MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro synchronizační informace.

“Monitorování a řízení kanálů v systému IBM i” na stránce 195

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

“Konfigurace připojení mezi serverem a klientem” na stránce 14

Chcete-li nakonfigurovat komunikační propojení mezi IBM MQ MQI clients a servery, rozhodněte se v komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

“Nastavení komunikace s ostatními správci front” na stránce 590

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS , které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

Související úlohy

“Konfigurace klastru správce front” na stránce 216

Klastry poskytují mechanismus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

Definování kanálů

Chcete-li odeslat zprávy z jednoho správce front do jiného, je třeba definovat dva kanály. Je třeba definovat jeden kanál ve zdrojovém správci front a jeden kanál v cílovém správci front.

Ve zdrojovém správci front

Definujte kanál s typem kanálu SENDER. Je třeba určit následující:

- Název přenosové fronty, která má být použita (atribut XMITQ).
- Název připojení partnerského systému (atribut CONNAME).
- Název komunikačního protokolu, který používáte (atribut TRPTYPE). V systému IBM MQ for z/OS musí být protokol protokolem TCP nebo LU6.2. Na ostatních platformách tuto volbu nemusíte zadávat. Můžete ji nechat pro výběr hodnoty z vaší výchozí definice kanálu.

Podrobnosti o všech atributech kanálu jsou uvedeny v části [Atributy kanálu](#).

V cílovém správci front

Definujte kanál s typem kanálu RECEIVER a se stejným názvem jako odesílací kanál.

Uvedte jméno komunikačního protokolu, který používáte (atribut TRPTYPE). V systému IBM MQ for z/OS musí být protokol protokolem TCP nebo LU6.2. Na ostatních platformách tuto volbu nemusíte zadávat. Můžete ji nechat pro výběr hodnoty z vaší výchozí definice kanálu.

Definice přijímacího kanálu mohou být generické. To znamená, že pokud máte několik správců front komunikujících se stejným příjemcem, odesílající kanály mohou pro příjemce zadat stejný název a pro všechny se použije jedna definice příjemce.

Definujete-li kanál, můžete jej otestovat pomocí příkazu PING CHANNEL. Tento příkaz odešle speciální zprávu z odesílacího kanálu do přijímacího kanálu a zkontroluje, zda je vrácena.

Poznámka: Hodnota parametru TRPTYPE je ignorována agentem oznamovacího kanálu zpráv. Např. TRPTYPE of TCP na definici kanálu odesílatele úspěšně začíná s TRPTYPE LU62 v definici kanálu příjemce jako partner.

Definování front

Chcete-li odesílat zprávy z jednoho správce front do jiného, je třeba definovat až šest front. Ve zdrojovém správci front je třeba definovat až čtyři fronty a až dvě fronty v cílovém správci front.

Ve zdrojovém správci front

- Definice vzdálené fronty

V této definici zadejte následující:

Název vzdáleného správce front

Název cílového správce front.

Název vzdálené fronty



Název cílové fronty v cílovém správci front.

Jméno přenosové fronty


Název přenosové fronty. Tento název přenosové fronty není třeba zadávat. Pokud ji nevytvoříte, použije se přenosová fronta se stejným názvem jako má cílový správce front. Pokud tato hodnota neexistuje, bude použita výchozí přenosová fronta. Doporučuje se, abyste přenosové frontě pojmenoval stejný název jako cílového správce front, aby byla fronta nalezena standardně.

- Definice inicializační fronty

 To je povinné. Musíte použít inicializační frontu s názvem SYSTEM.CHANNEL.INITQ.

  Toto je volitelné. Zvažte pojmenování inicializační fronty SYSTEM.CHANNEL.INITQ.

- Definice přenosové fronty

Lokální fronta s atributem USAGE nastaveným na XMITQ.  Pokud používáte nativní rozhraní IBM MQ for IBM i, atribut USAGE je *TMQ.

- Definice fronty nedoručených zpráv

Definujte frontu nedoručených zpráv, do které lze zapisovat nedoručené zprávy.

V cílovém správci front

- Definice lokální fronty

Cílová fronta. Název této fronty musí být stejný jako název fronty určené v poli názvu vzdálené fronty v definici vzdálené fronty ve zdrojovém správci front.

- Definice fronty nedoručených zpráv

Definujte frontu nedoručených zpráv, do které lze zapisovat nedoručené zprávy.

Související pojmy

[“Vytvoření přenosové fronty” na stránce 149](#)

Než bude možné spustit kanál (jiný než žadatelský kanál), musí být přenosová fronta definována tak, jak je popsáno v této sekci. Přenosová fronta musí být uvedena v definici kanálu.

[“Vytvoření přenosové fronty v systému IBM i” na stránce 149](#)

Přenosovou frontu na platformě IBM i můžete vytvořit pomocí panelu Vytvořit frontu MQM.

Vytvoření přenosové fronty

Než bude možné spustit kanál (jiný než žadatelský kanál), musí být přenosová fronta definována tak, jak je popsáno v této sekci. Přenosová fronta musí být uvedena v definici kanálu.

Definujte lokální frontu s atributem USAGE nastaveným na hodnotu XMITQ pro každý odesílající kanál zpráv. Chcete-li ve svých definicích vzdálených front použít určitou přenosovou frontu, vytvořte vzdálenou frontu podle následujícího obrázku.

Chcete-li vytvořit přenosovou frontu, použijte IBM MQ Commands (MQSC), jak je uvedeno v následujících příkladech:

Příklad příkazu pro vytvoření přenosové fronty

```
DEFINE QLOCAL(QM2) DESC('Transmission queue to QM2') USAGE(XMITQ)
```

Příklad příkazu pro vytvoření vzdálené fronty

```
DEFINE QREMOTE(PAYROLL) DESC('Remote queue for QM2') +  
XMITQ(QM2) RNAME(PAYROLL) RQMNAME(QM2)
```

Zvažte pojmenování přenosové fronty ve jménu správce front ve vzdáleném systému, jak je zobrazeno v příkladech.

Vytvoření přenosové fronty v systému IBM i

Přenosovou frontu na platformě IBM i můžete vytvořit pomocí panelu Vytvořit frontu MQM.

Musíte definovat lokální frontu s atributem pole Použití nastaveným na *TMQ, pro každý odesílající kanál zpráv.

Chcete-li použít definice vzdálených front, použijte stejný příkaz k vytvoření fronty typu *RMT a použítí *NORMAL.

Chcete-li vytvořit přenosovou frontu, použijte příkaz CRTMQMQ z příkazového řádku a zobrazí se vám první panel vytvoření fronty; viz [Obrázek 16 na stránce 150](#).

```

Create MQM Queue (CRTMQMQ)
Type choices, press Enter.
Queue name . . . . .
Queue type . . . . . ____ *ALS, *LCL, *MDL, *RMT
Message Queue Manager name . . . *DFT_____
-----

```

```

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
+

```

Obrázek 16. Vytvořit frontu (1)

Zadejte název fronty a určete typ fronty, který chcete vytvořit: Lokální, Vzdálený nebo Alias. V případě přenosové fronty zadejte na tomto panelu lokální (*LCL) a stiskněte klávesu Enter.

Zobrazí se druhá stránka panelu Vytvořit frontu MQM, viz [Obrázek 17 na stránce 150](#).

```

Create MQM Queue (CRTMQMQ)
Type choices, press Enter.
Queue name . . . . . > HURS.2.HURS.PRIORIT
Queue type . . . . . > *LCL *ALS, *LCL, *MDL, *RMT
Message Queue Manager name . . . *DFT
Replace . . . . . *NO *NO, *YES
Text 'description' . . . . .
Put enabled . . . . . *YES *SYSDFTQ, *NO, *YES
Default message priority . . . . 0 0-9, *SYSDFTQ
Default message persistence . . . *NO *SYSDFTQ, *NO, *YES
Process name . . . . .
Triggering enabled . . . . . *NO *SYSDFTQ, *NO, *YES
Get enabled . . . . . *YES *SYSDFTQ, *NO, *YES
Sharing enabled . . . . . *YES *SYSDFTQ, *NO, *YES

```

```

More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

Obrázek 17. Vytvořit frontu (2)

Změňte kteroukoli z výchozích zobrazených hodnot. Chcete-li přejít na další obrazovku, stiskněte klávesu Page Down, viz [Obrázek 18 na stránce 151](#).

Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

```
Default share option . . . . . *YES      *SYSDFTQ, *NO, *YES
Message delivery sequence . . . *PTY    *SYSDFTQ, *PTY, *FIFO
Harden backout count . . . . . *NO     *SYSDFTQ, *NO, *YES
Trigger type . . . . . *FIRST  *SYSDFTQ, *FIRST, *ALL...
Trigger depth . . . . . 1          1-99999999, *SYSDFTQ
Trigger message priority . . . . 0       0-9, *SYSDFTQ
Trigger data . . . . . '          '
Retention interval . . . . . 99999999 0-99999999, *SYSDFTQ
Maximum queue depth . . . . . 5000    1-24000, *SYSDFTQ
Maximum message length . . . . . 4194304 0-4194304, *SYSDFTQ
Backout threshold . . . . . 0         0-99999999, *SYSDFTQ
Backout requeue queue . . . . . '          '
Initiation queue . . . . . '          '

```

More...

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

Obrázek 18. Vytvořit frontu (3)

Zadejte *TMQ, pro přenosovou frontu, v poli Použití tohoto panelu a změňte kteroukoli z předvolených hodnot zobrazených v ostatních polích.

Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

```
Usage . . . . . *TMQ      *SYSDFTQ, *NORMAL, *TMQ
Queue depth high threshold . . . 80      0-100, *SYSDFTQ
Queue depth low threshold . . . 20     0-100, *SYSDFTQ
Queue full events enabled . . . *YES   *SYSDFTQ, *NO, *YES
Queue high events enabled . . . *YES   *SYSDFTQ, *NO, *YES
Queue low events enabled . . . *YES   *SYSDFTQ, *NO, *YES
Service interval . . . . . 99999999 0-99999999, *SYSDFTQ
Service interval events . . . . *NONE  *SYSDFTQ, *HIGH, *OK, *NONE
Distribution list support . . . *NO    *SYSDFTQ, *NO, *YES
Cluster Name . . . . . *SYSDFTQ
Cluster Name List . . . . . *SYSDFTQ
Default Binding . . . . . *SYSDFTQ *SYSDFTQ, *OPEN, *NOTFIXED

```

Bottom

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

Obrázek 19. Vytvořit frontu (4)

Jste-li spokojeni s tím, že pole obsahují správná data, stiskněte klávesu Enter a vytvořte frontu.

Spuštění kanálu

Při vkládání zpráv do vzdálené fronty definované ve zdrojovém správci front jsou tyto zprávy uloženy v přenosové frontě, dokud není kanál spuštěn. Po spuštění kanálu jsou zprávy doručovány do cílové fronty ve vzdáleném správci front.

Spusťte kanál v odesílajícím správci front pomocí příkazu START CHANNEL. Při spuštění odesílajícího kanálu je přijímající kanál automaticky spuštěn (modulem listener) a zprávy se odesílají do cílové fronty. Oba konce kanálu zpráv musí být spuštěny pro zprávy, které mají být přeneseny.

Vzhledem k tomu, že se oba konce kanálu nacházejí v různých správcích front, mohly být definovány s různými atributy. Chcete-li vyřešit všechny rozdíly, je počáteční vyjednávání dat mezi dvěma konci, když

se kanál spouští. Obecně platí, že oba konce kanálu pracují s atributy, které potřebují méně prostředků. To umožňuje větším systémům vyhovět menším prostředkům menších systémů na druhém konci kanálu zpráv.

Odesílající agent MCA rozdělí velké zprávy před jejich odesláním přes kanál. Jsou znovu složeny ve vzdáleném správci front. To není zřejmé uživateli.

Agent MCA může přenášet zprávy pomocí více podprocesů. Tento proces s názvem *pipelining* umožňuje agentovi MCA mnohem efektivněji přenášet zprávy s méně čekacími stavy. Potrubí zlepšuje výkon kanálu.

Řídicí funkce kanálu

Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

Příkazy jsou vydávány prostřednictvím panelů, programů nebo z příkazového řádku do řídicí funkce kanálu. Rozhraní panelu také zobrazuje stav kanálu a data definice kanálu. Programovatelné formáty příkazů nebo tyto příkazy IBM MQ (MQSC) a řídicí příkazy, které jsou podrobně popsány v produktu [“Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux”](#) na stránce 173, lze použít.

Příkazy spadají do následujících skupin:

- Administrace kanálu
- Řízení kanálů
- Monitorování stavu kanálu

Příkazy administrace kanálů se zabývají definicemi kanálů. Umožňují vám:

- Vytvořit definici kanálu
- Kopírování definice kanálu
- Změnit definici kanálu
- Odstranit definici kanálu

Příkazy pro řízení kanálů spravují činnost kanálů. Umožňují vám:

- Spustit kanál
- Zastavit kanál
- Znovu synchronizovat s partnerem (v některých implementacích)
- Resetovat pořadová čísla zpráv
- Vyřešit neověřnou dávku zpráv
- Ping: odeslání testovací komunikace přes kanál

Monitorování kanálů zobrazuje stav kanálů, například:

- Aktuální nastavení kanálu
- Zda je kanál aktivní nebo neaktivní
- Údaj o tom, zda kanál v synchronizovaném stavu byl ukončen

Další informace o definování, řízení a monitorování kanálů najdete v následujících dílčích tématech:

Příprava kanálů

Před pokusem o spuštění kanálu zpráv nebo kanálu MQI je třeba připravit kanál. Musíte se ujistit, že všechny atributy lokálních a vzdálených definic kanálů jsou správné a kompatibilní.

[Atributy kanálu](#) popisuje definice kanálů a atributy.

Ačkoli jste nastavili explicitní definice kanálů, vyjednávání o kanálu prováděná při spuštění kanálu může přepsat jednu nebo druhou z definovaných hodnot. Toto chování je normální a není zřejmé uživateli a bylo takto uspořádáno tak, aby jinak nekompatibilní definice mohly fungovat společně.

Automatická definice přijímacích kanálů a kanálů připojení k serveru

Pokud v produktu IBM MQ na všech platformách kromě z/OS neexistuje odpovídající definice kanálu, pak pro přijímač nebo kanál připojení serveru, který má povolenu automatickou definici, je definice vytvořena automaticky. Definice je vytvořena pomocí:

1. Vhodná definice kanálu modelu, SYSTEM.AUTO.RECEIVER nebo SYSTEM.AUTO.SVRCONN. Definice modelových kanálů pro automatickou definici jsou stejné jako výchozí nastavení systému, SYSTEM.DEF.RECEIVER a SYSTEM.DEF.SVRCONN, s výjimkou pole popisu, které je "Auto-definováno", následované 49 mezerami. Administrátor systému si může zvolit změnu libovolné části dodaných definic kanálů modelu.
2. Informace z partnerského systému. Hodnoty z partnera se použijí pro název kanálu a hodnotu zalomení pořadového čísla.
3. Ukončovací program kanálu, který můžete použít ke změně hodnot vytvořených funkcí auto-definition. Viz [Channel auto-definition exit program](#).

Popis je potom zkontrolován, aby se určilo, zda byl změněn při ukončení automatické definice, nebo protože definice modelu byla změněna. Pokud je první 44 znaků stále "Automaticky definováno" následovaným počtem 29 mezer, přidá se název správce front. Pokud posledních 20 znaků je stále ve všech mezerevých znacích, přidá se místní čas a datum.

Když byla definice vytvořena a uložena, pokračuje se při spuštění kanálu, jako by definice vždy existovala. Velikost dávky, velikost přenosu a velikost zprávy se vyjednává s partnerem.

Definování jiných objektů

Před spuštěním kanálu zpráv musí být oba konce ve svých správcích front definovány (nebo povoleny pro automatickou definici). Přenosová fronta, kterou má sloužit, musí být definována pro správce front na odesílajícím konci. Komunikační spojení musí být definováno a dostupné. Může být nezbytné připravit další objekty produktu IBM MQ, jako jsou definice vzdálených front, definice aliasů správce front a definice alias fronty pro odpověď, k implementaci scénářů popsaných v tématu ["Konfigurace distribuovaných front"](#) na stránce 124.

Informace o definování kanálů MQI viz ["Definování kanálů MQI"](#) na stránce 28.

Více kanálů zpráv na přenosovou frontu

Je možné definovat více než jeden kanál na přenosovou frontu, ale pouze jeden z těchto kanálů může být aktivní v jednom okamžiku. Zvažte použití této volby pro zajišťování alternativních tras mezi správci front pro vyvážení provozu a akce nápravného připojení k selhání propojení. Přenosová fronta nemůže být použita jiným kanálem, pokud předchozí kanál k jeho použití ukončil v nejistém stavu odeslání dávky zpráv na odesílajícím konci. Další informace viz ["Nejisté kanály"](#) na stránce 163.

Spuštění kanálu

Kanál může být způsoben k zahájení přenosu zpráv jedním ze čtyř způsobů. Může být:

- Spuštěno operátorem (nikoli přijímačem, přijímačem klastru nebo kanály připojení serveru).
- Spuštěno z přenosové fronty. Tato metoda se vztahuje pouze na odesílací kanály a plně kvalifikované kanály serveru (kanály, které určují pouze CONNAME). Musíte připravit potřebné objekty pro spouštěcí kanály.
- Spouští se z aplikačního programu (nikoli z přijímačů, přijímačů klastru nebo kanálu připojení serveru).
- Spouští se vzdáleně ze sítě odesílatelem, odesílatelem klastru, klientem, serverem nebo kanálem připojení klienta. Přijímací přijímače, přijímače klastru a pravděpodobně i serverový a žadatelský kanál

jsou tímto způsobem spuštěny; takže se jedná o kanály připojení serveru. Samotné kanály již musí být spuštěny (to znamená povoleno).

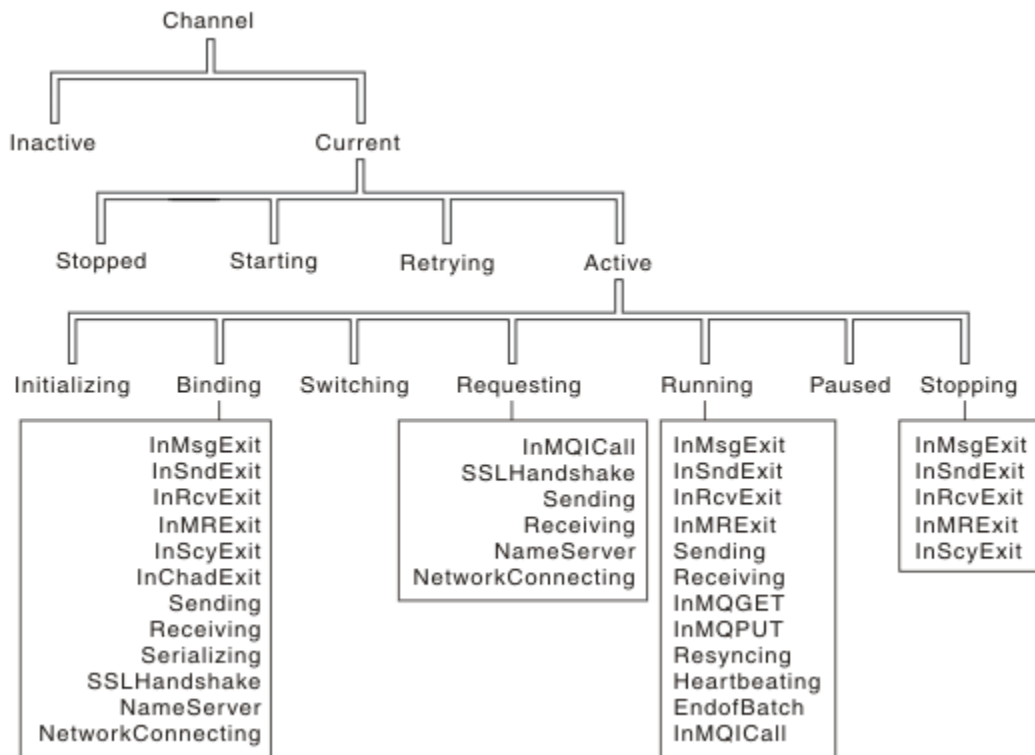
Poznámka: Vzhledem k tomu, že kanál je 'spuštěn', nemusí nutně přenášet zprávy. Místo toho může být 'povoleno' spustit přenos, když se vyskytne jedna ze čtyř událostí popsaných dříve. Povolení a zakázání kanálu je dosaženo pomocí příkazů operátorů START a STOP.

Stavy kanálů

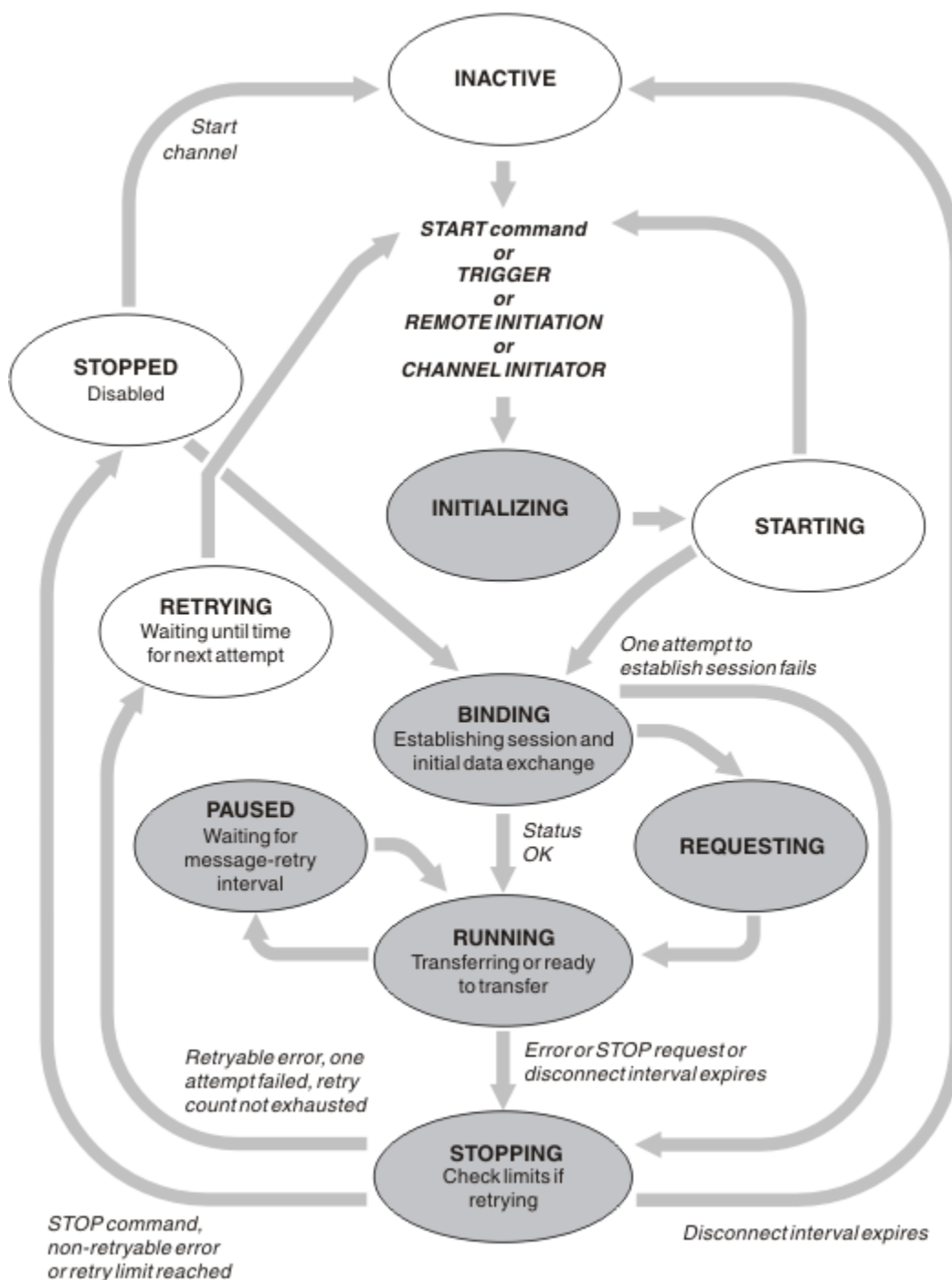
Kanál může být v libovolném okamžiku v některém z mnoha stavů. Některé stavy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

Obrázek 20 na stránce 154 zobrazuje hierarchii všech možných stavů kanálů a podstavů, které se vztahují ke každému z kanálů kanálu.

Obrázek 21 na stránce 155 zobrazuje odkazy mezi stavy kanálů. Tyto odkazy se vztahují na všechny typy kanálů zpráv a kanálů připojení k serveru.



Obrázek 20. Stavy kanálů a podstavy



Obrázek 21. Toky mezi stavy kanálů

Aktuální a aktivní

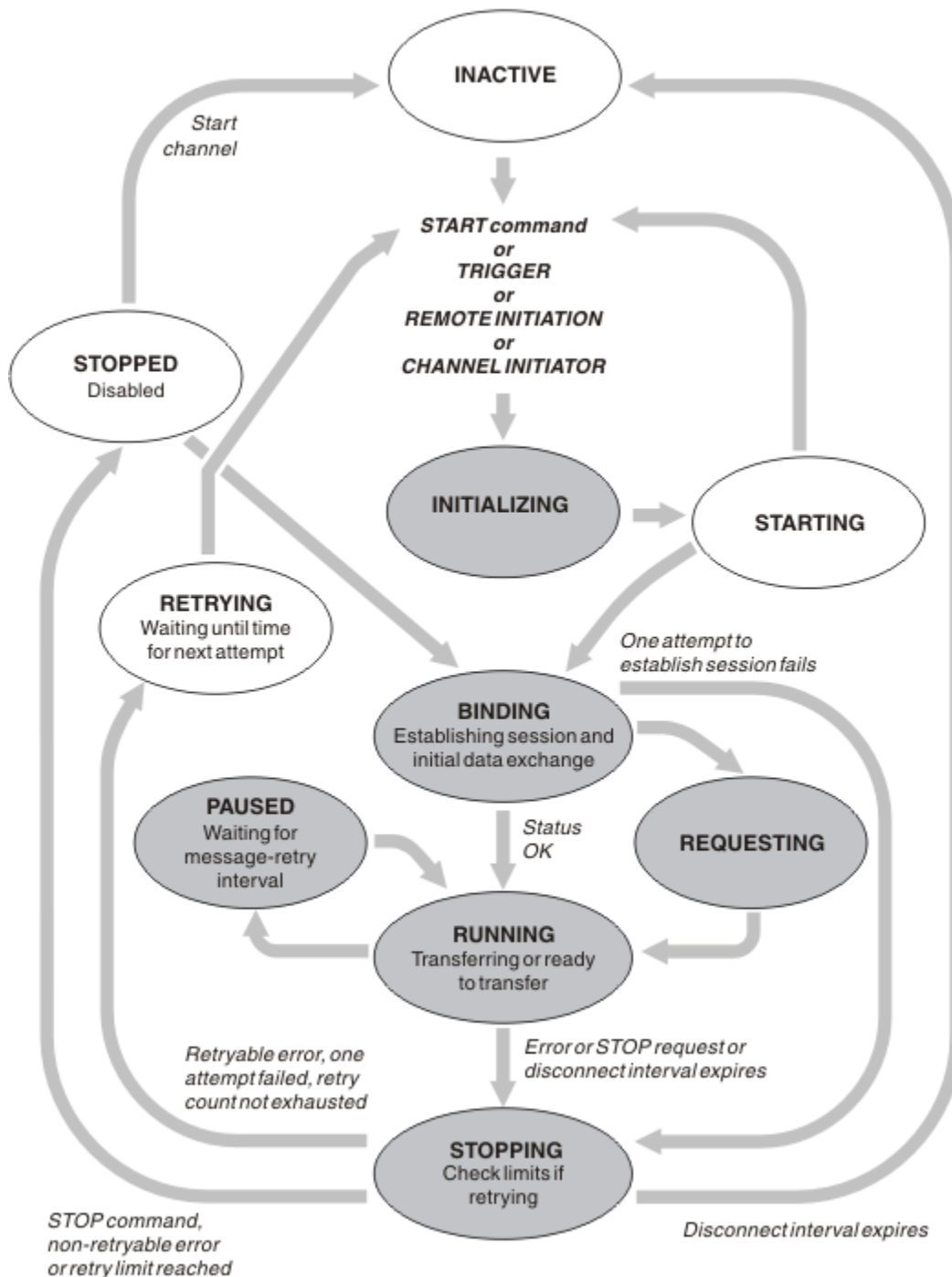
Kanál je *aktuální*, je-li ve stavu jiném než neaktivní. Aktuální kanál je *aktivní*, pokud není ve stavu RETRYING, STOPPED nebo STARTING. Je-li kanál aktivní, je spotřebovávat prostředky a je spuštěn proces nebo podproces. Sedm možných stavů aktivního kanálu (INITIALIZING, BINDING, SWITCHING, REQUESTING, RUNNING, PAUSED nebo STOPPING) jsou zvýrazněny v [Obrázek 21 na stránce 155](#).

Aktivní kanál může také zobrazit podstav poskytující více podrobností přesně toho, co kanál dělá. Podstavy pro každý stav jsou zobrazeny v [Obrázek 20 na stránce 154](#).

Aktuální a aktivní

Kanál je "aktuální", je-li ve stavu jiném než neaktivní. Aktuální kanál je "aktivní", pokud není ve stavu RETRYING, STOPPED nebo STARTING.

Je-li kanál "aktivní", může také zobrazit podstav poskytující více podrobností přesně toho, co kanál dělá.







Obrázek 22. Toky mezi stavy kanálů

Poznámka:

1. Je-li kanál v jednom ze šesti stavů zvýrazněných v Obrázek 22 na stránce 156 (INITIALIZING, BINDING, REQUESTING, RUNNING, PAUSED nebo STOPPING), spotřebovává se prostředek a je spuštěn proces nebo podproces; kanál je *aktivní*.
2. Je-li kanál ve stavu ZASTAVENO, může být relace aktivní, protože další stav zatím není znám.

Určení maximálního počtu aktuálních kanálů

Můžete uvést maximální počet kanálů, které mohou být aktuální v daném okamžiku. Toto číslo je počet kanálů, které mají položky ve stavové tabulce kanálu, včetně kanálů, které se opakují, a kanálů, které jsou zastaveny. Tuto volbu uveďte pomocí  ALTER QMGR MAXCHL pro z/OS,  Inicializační soubor správce front pro IBM i, konfigurační soubor správce front pro systémy SYSTÉM UNIX a Linux nebo MQ Explorer. Další informace o hodnotách nastavených pomocí inicializačního programu nebo konfiguračního souboru naleznete v tématu [Stanzy konfiguračního souboru pro distribuované řazení do fronty](#). Další informace o určení maximálního počtu kanálů viz [Administrace IBM MQ pro systémy IBM MQ for UNIX a Linux a systémy Windows](#) , [Administrace IBM i for IBM MQ for IBM i](#) , nebo [Administrace IBM MQ for z/OS pro IBM MQ for z/OS](#) .

Poznámka:

1. Kanály připojení serveru jsou zahrnuty v tomto počtu.
2. Kanál musí být aktuální, dříve než může být aktivní. Pokud je kanál spuštěn, ale nemůže se stát aktuální, spuštění se nezdaří.

Určení maximálního počtu aktivních kanálů


Můžete také uvést maximální počet aktivních kanálů, abyste zabránili přetížení systému mnoha spouštěnými kanály. Použijete-li tuto metodu, nastavte atribut intervalu odpojení na nízkou hodnotu, aby bylo možné spustit čekání kanálů, jakmile budou ukončeny další kanály.

Pokaždé, když se kanál, který se opakovaně pokouší navázat spojení s partnerem, stane aktivním kanálem, musí se stát aktivním kanálem. Pokud dojde k selhání pokusu, zůstane aktuální kanál, který není aktivní, dokud se nepokusí o další pokus. Počet opakovaných pokusů kanálu a četnost, která je určena počtem opakování a atributy kanálu intervalu opakování opakování. Pro oba tyto atributy existují krátké a dlouhé hodnoty. Další informace naleznete v tématu [Atributy kanálu](#) .

Když se kanál musí stát aktivním kanálem (protože byl vydán příkaz START nebo proto, že byl spuštěn nebo protože nastal čas pro další pokus o zopakování), ale nelze tak učinit, protože počet aktivních kanálů je již na maximální hodnotě, kanál čeká, dokud nebude jeden z aktivních slotů uvolněn jinou instancí kanálu, která přestane být aktivní. Pokud se však kanál spouští, protože je spuštěn vzdáleně, a v té době nejsou k dispozici žádné aktivní sloty, je vzdálené zahájení zamítnuto.



Kdykoli se kanál, který je jiný než žadatelský kanál, pokouší stát se aktivním, přejde do stavu STARTING. Tento stav se vyskytuje i v případě, že je aktivní slot okamžitě dostupný, i když je ve stavu STARTING pouze krátkou dobu. Pokud však musí kanál čekat na aktivní slot, je ve stavu STARTING, zatímco čeká.

Kanály žadatele nepůjdou do stavu STARTING. Pokud nelze spustit žadatelský kanál, protože počet aktivních kanálů je již na limitu, kanál se ukončí nestandardně.

Kdykoli kanál, který není žadatelovým kanálem, nedokáže získat aktivní slot, a tak čeká na první zprávu, zapíše se zpráva do protokolu  nebo konzole z/OS , a vygeneruje se událost. Je-li slot později uvolněn a kanál je schopen získat, vygeneruje se další zpráva a událost. Ani jedna z těchto událostí a zpráv se negeneruje, je-li kanál schopen přímo získat slot.

Je-li příkaz STOP CHANNEL zadán v době, kdy kanál čeká na aktivaci, kanál přejde do stavu STOPPED. Vyzvedne se událost Kanál-Stopped.


Kanály připojení k serveru jsou zahrnuty v maximálním počtu aktivních kanálů.

Další informace o určení maximálního počtu aktivních kanálů viz [Administrace IBM MQ pro systémy IBM MQ for UNIX a Linux a systémy Windows](#) , [Administrace IBM i for IBM MQ for IBM i](#) , nebo [Administrace IBM MQ for z/OS pro IBM MQ for z/OS](#) .


Chyby kanálu


Chyby na kanálech způsobí, že kanál zastaví další přenosy. Je-li kanálem odesílatel nebo server, přejde do stavu RETRY, protože je možné, že se problém může vymazat sám. Pokud nelze přejít do stavu RETRY, kanál přejde do stavu ZASTAVENO.

V případě posílání kanálů je přidružená přenosová fronta nastavena na GET (DISABLED) a spuštění je vypnuto. (Příkaz STOP s hodnotou STATUS (STOPPED) převezme stranu, která ji vydala do stavu ZASTAVENO; pouze expirace intervalu odpojení nebo příkazu STOP s hodnotou STATUS (INACTIVE) jej ukončí normálně a stane se neaktivním.) Kanály, které jsou ve stavu ZASTAVENO, potřebují zásah operátora, než se mohou znovu spustit (viz [“Restartování zastavených kanálů”](#) na stránce 162).

Poznámka: Pro systémy  IBM i, UNIX, Linux a Windows musí být spuštěn inicializátor kanálu, aby se pokus o pokus o pokus pokusil. Není-li inicializátor kanálu k dispozici, bude kanál neaktivní a musí být restartován ručně. Pokud používáte skript ke spuštění kanálu, ujistěte se, že inicializátor kanálu je spuštěn před tím, než se pokusíte spustit skript.

[Počet dlouhých opakování \(LONGRTY\)](#) popisuje, jak probíhá opakování prací. Je-li chyba vymazána, kanál se restartuje automaticky a přenosová fronta je znovu povolena. Je-li dosažen limit opakování bez vymazání chyby, kanál přejde do stavu ZASTAVENO. Zastavený kanál musí být ručně restartován operátorem. Je-li chyba stále přítomna, neopakuje pokus znovu. Když se úspěšně spustí, přenosová fronta je znovu povolena.

 Pokud se inicializátor kanálu zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu inicializátoru kanálu. Stav kanálu pro typ kanálu SVRCONN se však resetuje, pokud se zastaví inicializátor kanálu v době, kdy je kanál ve stavu ZASTAVENO.

 Pokud se správce front zastaví v případě, že se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu správce front. Od verze IBM MQ 8.0 se tato vztahuje také na kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

Pokud kanál nemůže vložit zprávu do cílové fronty, protože je tato fronta plná nebo byla zablokována, může kanál zopakovat operaci (uvedený v atributu počtu opakování zprávy) v časovém intervalu (uvedený v atributu intervalu opakování zprávy). Případně můžete napsat vlastní proceduru opakování zpráv, která určuje, které okolnosti způsobí opakovaný pokus, a počet provedených pokusů. Kanál přejde do stavu PAUSED při čekání na dokončení intervalu opakování zprávy.

Chcete-li získat informace o atributech kanálu a o [Kanály-uživatelské programy pro kanály systému zpráv](#) informace o ukončení opakování zprávy, prohlédněte si příručku [Atributy kanálu](#) a informace o nich.

Limity kanálu připojení serveru

Můžete nastavit limity kanálu připojení k serveru, které zabrání klientským aplikacím v vyčerpání prostředků kanálu správce front, **MAXINST** a zabránit tak, aby jedna klientská aplikace byla vyčerpána kapacita kanálu připojení serveru **MAXINSTC**.

Nastavili jste **MAXINST** a **MAXINSTC** příkazem **DEFINE CHANNEL** .

Maximální celkový počet kanálů může být v každém okamžiku ve správci front aktivní. Celkový počet instancí kanálu připojení serveru je zahrnut v maximálním počtu aktivních kanálů.

Nezadáte-li maximální počet současně existujících instancí kanálu připojení serveru, který lze spustit, je možné použít jedinou klientskou aplikaci, která se připojuje k jednomu kanálu připojení serveru, aby vyčerpala maximální počet aktivních kanálů, které jsou k dispozici. Když je dosaženo maximálního počtu aktivních kanálů, zabrání spuštění jakýchkoli jiných kanálů ve správci front. Chcete-li se této situaci vyhnout, musíte omezit počet souběžných instancí jednotlivého kanálu připojení serveru, který může být spuštěn bez ohledu na to, který klient je spustil.

Je-li hodnota limitu omezena na pod aktuálně spuštěným počtem instancí kanálu pro připojení k serveru, dokonce i na nulu, spuštěné kanály nebudou ovlivněny. Nové instance nelze spustit, dokud nebudou úspěšně spuštěny dostatečné existující instance, takže počet momentálně spuštěných instancí je menší než hodnota limitu.

Mnoho různých kanálů připojení klienta se také může připojit k jednotlivým kanálům připojení serveru. Limit počtu současných instancí jednotlivého kanálu připojení serveru, který může být spuštěn bez ohledu na to, který klient je spustil, zabrání klientovi v vyčerpání maximální kapacity aktivního kanálu správce front. Pokud také neomezíte počet simultánních instancí jednotlivých kanálů připojení k serveru, které lze spustit z jednoho klienta, pak je možné, aby jedna, vadná klientská aplikace otevřela tolik připojení, že vyčerpá kapacitu kanálu alokovanou pro jednotlivé kanály připojení serveru, a zabrání tak dalším klientům, kteří potřebují připojení k tomuto kanálu, aby mohli používat kanál. Chcete-li se této situaci vyhnout, je třeba omezit počet současně existujících instancí jednotlivých kanálů připojení serveru, které lze spustit z jednotlivých klientů.

Je-li hodnota individuálního limitu klienta redukována pod počet instancí kanálu připojení serveru, které momentálně běží od jednotlivých klientů, dokonce i na nulu, spuštěné kanály nejsou ovlivněny. Nové instance kanálu připojení serveru však nelze spustit z jednoho klienta, který překračuje nový limit, dokud nebudou spuštěné dostatečné existující instance z tohoto klienta, takže počet momentálně spuštěných instancí je menší než hodnota tohoto parametru.

Související informace

[Atributy kanálu a typy kanálů](#)

[Definovat kanál](#)

Kontrola, zda je druhý konec kanálu stále k dispozici

Můžete použít interval prezenčního signálu, interval udržení aktivity a časový limit příjmu, abyste zkontrolovali, zda je druhý konec kanálu dostupný.

Prezenční signály

Pomocí atributu kanálu intervalu prezenčního signálu můžete určit, že toky mají být předávány z odesílající sběrnice MCA v případě, že v přenosové frontě nejsou žádné zprávy, jak je popsáno v tématu [Interval prezenčního signálu \(HBINT\)](#).

Trvání platnosti

Pokud v produktu IBM MQ for z/OS používáte protokol TCP/IP jako přenosový protokol, můžete také zadat hodnotu pro atribut kanálu intervalu produktu **Keepalive** (KAIN). Doporučuje se, abyste časový interval **Keepalive** poskytli vyšší hodnotu než interval prezenčního signálu a nižší hodnotu než hodnota odpojení. Tento atribut můžete použít k určení hodnoty časového limitu pro každý kanál, jak je popsáno v tématu [Interval udržení aktivity \(KAIN\)](#).

Pokud používáte protokol TCP jako přenosový protokol, v produktu IBM MQ pro systémy IBM i, SYSTÉM UNIX, Linux a Okna můžete nastavit `keepalive=yes`. Uvedete-li tuto volbu, TCP bude pravidelně kontrolovat, zda je druhý konec připojení stále dostupný. Není-li kanál ukončen, kanál se ukončí. Tato volba je popsána v části [Interval udržení aktivity \(KAIN\)](#).

Máte-li nespolehlivé kanály, které hlásí chyby TCP, znamená to, že použití volby **Keepalive** znamená, že se vaše kanály budou pravděpodobně zotavovat.

Můžete zadat časové intervaly, které budou řídit chování volby **Keepalive**. Změníte-li časový interval, budou ovlivněny pouze kanály TCP/IP spuštěné po změně časového intervalu. Ujistěte se, že hodnota, kterou jste vybrali pro časový interval, je menší než hodnota intervalu odpojení pro kanál.

Další informace o použití volby **Keepalive** naleznete v parametru [KAIN](#) v příkazu [DEFINE CHANNEL](#).

Časový limit pro příjem

Používáte-li protokol TCP jako přenosový protokol, bude při příjmu nečinného připojení kanálu mimo rozhraní MQI také ukončeno, pokud nejsou přijata žádná data po určitou dobu. Toto období, hodnota *prodlevy příjmu*, je určeno podle hodnoty HBINT (Preartbeat interval).

V systémech IBM MQ pro systémy IBM i, SYSTÉM UNIX, Linux a Okna je hodnota *vypršení časového limitu příjmu* nastavena takto:

1. Pro počáteční počet toků před každým dohadováním je hodnota *time-out* dvojnásobná než hodnota HBINT z definice kanálu.
2. Poté, co kanály vyjednájí hodnotu HBINT, je-li hodnota HBINT nastavena na hodnotu menší než 60 sekund, nastaví se hodnota proměnné *receive time-out* na hodnotu dvojnásobku této hodnoty. Je-li hodnota HBINT nastavena na 60 sekund nebo vyšší, je hodnota *vypršení časového limitu příjmu* nastavena na hodnotu 60 sekund větší než hodnota HBINT.

V produktu IBM MQ for z/OS je hodnota *vypršení časového limitu pro příjem* nastavena takto:

1. Pro počáteční počet toků před každým dohadováním je hodnota *time-out* dvojnásobná než hodnota HBINT z definice kanálu.
2. Je-li nastavena volba RCVTIME, časový limit je nastaven na jednu z následujících hodnot:
 - vyjednaná hodnota HBINT vynásobená konstantou
 - vyjednaná HBINT plus konstantní počet sekund
 - konstantní počet sekund

v závislosti na parametru RCVTTYPE a s výhradou omezení stanoveného RCVTMIN, pokud se použije. RCVTMIN se nepoužije, je-li konfigurován parametr RCVTTYPE (EQUAL). Pokud použijete konstantní hodnotu RCVTIME a používáte interval prezenčního signálu, neuvádějte RCVTIME menší než interval prezenčního signálu. Podrobnosti o atributech RCVTIME, RCVTMIN a RCVTTYPE najdete v popisu příkazu ALTER QMGR.

Poznámka:

1. Je-li jedna z hodnot nulová, neexistuje žádný časový limit.
2. U připojení, která nepodporují prezenční signály, se hodnota HBINT v kroku 2 vyjednává k nule, a proto není nastaven žádný časový limit, takže musíte použít rozhraní TCP/IP KEEPALIVE.
3. U připojení klienta, které používají konverzace sdílení, mohou prezenční signály proudit přes kanál (z obou konců) po celou dobu, nejen když je operace MQGET nevyřízenou.
4. U připojení klienta, u kterých se nepoužívá sdílení konverzací, jsou prezenční signály odesílány ze serveru pouze v případě, že klient odešle volání MQGET s čekáním. Proto se nedoporučuje nastavit interval prezenčního signálu pro kanály klienta příliš malý. Je-li například prezenční signál nastaven na 10 sekund, volání MQCMIT selže (příkazem MQRC_CONNECTION_BROKEN), trvá-li déle než 20 sekund, protože během této doby nedošlo k žádnému toku dat. To se může stát s velkými jednotkami práce. Nestane se však, pokud jsou zvoleny odpovídající hodnoty pro interval prezenčního signálu, protože pouze operace MQGET s čekáním trvá příliš dlouhá časová období.

Poskytnutá hodnota SHARECNV není nulová, klient používá úplné duplexní připojení, což znamená, že klient může (a provádí) prezenční signál během všech volání MQI.

5. V kanálech klienta produktu IBM MQ verze 7 mohou prezenční signály procházet jak z serveru, tak i z klientské strany. Časový limit na obou koncích je založen na hodnotě $2 \cdot \text{HBINT}$ pro HBINTS menší než 60 sekund a $\text{HBINT} + 60$ pro HBINTS po dobu delší než 60 sekund.
6. Zrušení připojení po dvojnásobku intervalu prezenčního signálu je platné, protože tok dat nebo prezenční signál je očekáván alespoň při každém intervalu prezenčního signálu. Nastavení intervalu prezenčního signálu je však příliš malé, může však způsobit problémy, zvláště pokud používáte uživatelské procedury kanálu. Je-li například hodnota HBINT jedna sekunda a je-li použita uživatelská procedura pro odeslání nebo přijetí, bude přijímající koncový systém čekat pouze 2 sekundy před zrušením kanálu. Pokud agent MCA provádí úlohu, jako je např. šifrování zprávy, může být tato hodnota příliš krátká.

Převzetí agenta MCA

Funkce Převzetí agenta MCA umožňuje produktu IBM MQ zrušit přijímací kanál a spustit nový na jeho místě.

Pokud kanál ztratí kontakt, kanál příjemce může být ponechán ve stavu 'příjem komunikace'. Když je komunikace znovu zavedena, kanál odesílatele se pokusí znovu navázat spojení. Pokud vzdálený správce

front zjistí, že je kanál příjemce již spuštěn, nebude moci spustit jinou verzi téhož kanálu příjemce. Tento problém vyžaduje zásah uživatele k nápravě problému nebo použití systému keepalive.

Funkce Převzetí MCA řeší problém automaticky. Umožňuje IBM MQ kanálu příjemce zrušit kanál příjemce a spustit nový jeho místo.

Funkci lze nastavit s různými volbami:

- **distributed** Na distribuovaných platformách najdete informace v tématu [Administrace produktu IBM MQ](#).
- **z/OS** Pro z/OS viz [Administrace IBM MQ for z/OS](#).
- **IBM i** Pro IBM i viz [Administrace IBM i](#).

Zastavení a uvedení kanálů do klidového stavu

Kanál můžete zastavit a uvést do klidového stavu před vypršením časového intervalu odpojení.

Kanály zpráv jsou navrženy tak, aby byly přerušitelné spojení mezi správcí front se spořádaným ukončením řízeným pouze atributem kanálu přerušeni připojení. Tento mechanismus funguje dobře, pokud operátor nemusí před vypršením časového intervalu odpojení ukončit kanál. K této potřebě může dojít v následujících situacích:

- Uvedení do klidu
- Ochrana prostředků
- Jednostranná akce na jednom konci kanálu

V takovém případě můžete kanál zastavit. Můžete to provést pomocí:

- v příkazu STOP CHANNEL MQSC
- příkaz Stop Channel PCF
- Průzkumník IBM MQ
- **IBM i** **z/OS** jiné mechanismy specifické pro jednotlivé platformy:

z/OS **Pro z/OS:**
Panel Zastavení kanálu

IBM i **Pro IBM i:**
CL příkaz ENDMQMCHL nebo parametr END na panelu WRKMQMCHL

Pro zastavení kanálů pomocí těchto příkazů jsou k dispozici tři možnosti:

QUIESCE

Volba QUIESCE se pokouší ukončit aktuální dávku zpráv před zastavením kanálu.

Vynutit

Volba FORCE se pokouší okamžitě zastavit kanál a může vyžadovat opětovnou synchronizaci kanálu při restartu, protože kanál může být ponechán na pochybách.

z/OS V systému IBM MQ for z/OS FORCE přeruší probíhající opětovné přidělení zpráv, což může zanechat BIND_NOT_FIXED zpráv částečně přelokovaná nebo mimo pořadí.

TERMINATE

Volba TERMINATE se pokouší zastavit kanál okamžitě a ukončí vlákno nebo proces kanálu.

z/OS V systému IBM MQ for z/OS TERMINATE přeruší probíhající opětovné přidělení zpráv, což může zanechat BIND_NOT_FIXED zprávy částečně přelokovaná nebo mimo pořadí.

Všechny tyto volby opustí kanál ve stavu STOPPED, které vyžadují zásah operátora k jeho restartování.

Zastavení kanálu na odesílajícím konci je efektivní, ale vyžaduje zásah operátora k restartování. Na přijímajícím konci kanálu jsou věci mnohem obtížnější, protože agent MCA čeká na data z odesílající strany

a neexistuje žádný způsob, jak zahájit *spořádaný* ukončení kanálu z přijímající strany; příkaz pro zastavení bude nevyřízený až do doby, než se agent MCA vrátí z dat.

V důsledku toho existují tři doporučené způsoby použití kanálů v závislosti na požadovaných provozních charakteristikách:

- Chcete-li, aby vaše kanály byly přerušitelné, uvědomte si, že může dojít k řádnému ukončení pouze z odesílajícího konce. Když jsou kanály přerušeny, je to zastaveno, je nutný zásah operátora (příkaz START CHANNEL), aby je bylo možné restartovat.
- Chcete-li, aby byly kanály aktivní pouze v případě, že pro ně existují zprávy, které mají být přeneseny, nastavte interval odpojení na poměrně nízkou hodnotu. Výchozí nastavení je vysoké, a proto se nedoporučuje pro kanály, kde je tato úroveň řízení požadována. Vzhledem k tomu, že je obtížné přerušit přijímacího kanálu přerušovat, je nejhospodárnější volbou kanál automaticky odpojit a znovu se připojit, jak se pracovní zátěž vyžaduje. U většiny kanálů může být vhodné nastavení intervalu odpojení heuristicky vytvořeno.
- Pomocí atributu intervalu prezenčního signálu můžete způsobit, že odesílající agent MCA odešle tok synchronizačních signálů do přijímajícího agenta MCA během období, ve kterém nemá žádné zprávy k odeslání. Tato akce uvolní přijímajícího agenta MCA ze svého stavu čekání a dává mu možnost uvést kanál do klidového stavu bez čekání na vypršení časového limitu odpojení. Nastavte interval prezenčního signálu o nižší hodnotu, než je hodnota intervalu odpojení.



Poznámka:

1. Doporučuje se nastavit interval odpojení na nízkou hodnotu, nebo použít prezenční signály pro kanály serveru. Tato nízká hodnota znamená povolení pro případ, kdy se kanál žadatele ukončí abnormálně (například proto, že kanál byl zrušen), když nejsou k dispozici žádné zprávy pro kanál serveru k odeslání. Je-li interval odpojení nastaven na vysoké a prezenční signály se nepoužívají, server nedetekuje, že žadatel skončil (což bude provádět pouze při příštím pokusu o odeslání zprávy žadateli). Je-li server stále spuštěn, má otevřenou přenosovou frontu pro výhradní vstup, aby bylo možné získat další zprávy, které dorazí do fronty. Je-li učiněn pokus o restartování kanálu od žadatele, požadavek na spuštění obdrží chybu, protože server má stále otevřenou přenosovou frontu pro výhradní vstup. Je třeba zastavit kanál serveru a poté znovu spustit kanál z klienta.


Restartování zastavených kanálů


Když kanál přejde do stavu STOPPED, je nutné kanál restartovat ručně.

Kanál můžete restartovat následujícími způsoby:

- Pomocí příkazu **START CHANNEL MQSC**.
- Pomocí příkazu **Start Channel PCF**.
- Pomocí produktu MQ Explorer.
-  V systému z/OS pomocí panelu Spustit kanál.
-  V systému IBM i pomocí příkazu **STRMQMCHL CL** nebo volby **ZAČÁTEK** na panelu WRKMQMCHL.

V případě odesílatelů nebo kanálů serveru, kdy kanál vstoupil do stavu STOPPED, byla přidružená přenosová fronta nastavena na GET (DISABLED) a spuštění bylo vypnuto. Když je přijat požadavek na spuštění, tyto atributy se resetují automaticky.

 Pokud se inicializátor kanálu zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu inicializátoru kanálu. Stav kanálu pro typ kanálu SVRCONN se však resetuje, pokud se zastaví inicializátor kanálu v době, kdy je kanál ve stavu ZASTAVENO.

 Pokud se správce front zastaví v případě, že se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu správce front. Počínaje verzí IBM MQ Verze 8.0 se tato volba vztahuje také na kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

Nejisté kanály

Pochybný kanál je kanál, který má pochybnosti se vzdáleným kanálem o tom, které zprávy byly odeslány a přijaty.

Všimněte si, že rozdíl mezi tímto a správcem front je nejistý o tom, které zprávy by měly být potvrzeny do fronty.

Pomocí parametru kanálu Dávkový prezenční signál (BATCHHB) můžete snížit příležitost pro kanál, který má být umístěn v nejistém stavu. Je-li zadána hodnota tohoto parametru, kanál odesílatele před provedením dalších akcí kontroluje, zda je vzdálený kanál ještě aktivní. Pokud není přijata žádná odezva, kanál příjemce se považuje za již neaktivní. Zprávy lze odvolat, znovu směřovat a odesílací kanál nepochybuje. To snižuje dobu, kdy může být kanál umístěn v nejistém stavu mezi odesílacím kanálem, který ověřuje, zda je kanál příjemce stále aktivní, a ověřením, zda kanál příjemce obdržel odeslané zprávy. Další informace o parametru prezenčního signálu dávky naleznete v tématu [Atributy kanálu](#).

Problémy s nejistým kanálem se obvykle řeší automaticky. I když je komunikace ztracena a kanál je umístěn v nejistém stavu s dávkou zprávy u odesílatele s neznámým stavem příjmy, je situace vyřešena při opětovném navázání komunikace. Záznamy pořadových čísel a LUWID jsou uchovány pro tento účel. Kanál bude nejistý, dokud nebudou vyměněny informace o LUWID a pouze jedna dávka zpráv může mít pochybnosti o kanálu.

Je-li to nezbytné, můžete kanál znovu synchronizovat ručně. Termín *ruční* zahrnuje použití operátorů nebo programů, které obsahují příkazy správy systému IBM MQ. Proces ruční synchronizace funguje následujícím způsobem. Tento popis používá příkazy MQSC, ale můžete také použít ekvivalenty PCF.

1. Použijte příkaz DISPLAY CHSTATUS k vyhledání poslední potvrzené logické pracovní jednotky ID (LUWID) pro **každou** stranu kanálu. Toto proveďte pomocí následujících příkazů:

- Pro nejistou stranu kanálu:

```
DISPLAY CHSTATUS( name ) SAVED CURLUWID
```

Pro další identifikaci kanálu můžete použít parametry CONNAME a XMITQ.

- Pro přijímající stranu kanálu:

```
DISPLAY CHSTATUS( name ) SAVED LSTLUWID
```

Parametr CONNAME můžete použít k dalšímu označení kanálu.

Příkazy jsou odlišné, protože pouze odesílající strana kanálu může být nejistá. Přijímající strana není nikdy na pochybách.

V systému IBM MQ for IBM ilze příkaz DISPLAY CHSTATUS spustit ze souboru pomocí příkazu STRMQMOMQSC nebo pomocí příkazu Práce se stavem kanálu MQM na příkazu WRKMQMCHST.

2. Jsou-li dvě jednotky LUWID stejné, přijímající strana spáchala jednotku práce, kterou odesílatel považuje za nejistou. Odesílající strana nyní může odstranit nejisté zprávy z přenosové fronty a znovu ji povolit. To se provádí s následujícím příkazem kanálu RESOLVE:

```
RESOLVE CHANNEL( name ) ACTION(COMMIT)
```

3. Pokud se obě LUWID liší, přijímající strana nepotvrdila jednotku práce, kterou odesílatel považuje za nejistou. Odesílající strana musí uchovávat nejisté zprávy v přenosové frontě a znovu je odeslat. To se provádí s následujícím příkazem kanálu RESOLVE:

```
RESOLVE CHANNEL( name ) ACTION(BACKOUT)
```

 V systému IBM MQ for IBM můžete použít příkaz Vyřešit kanál MQM, RSVMQMCHL.

Jakmile je tento proces dokončen, kanál již není na pochybách. V případě potřeby může být přenosová fronta v případě potřeby použita jiným kanálem.

Určování problémů

Při určování problémů se vyskytují dva různé aspekty-problémy zjištěné při odeslání příkazu a problémy zjištěné během provozu kanálů.

Ověření příkazu

Příkazy a data panelu musí být bez chyb, než jsou přijaty ke zpracování. Jakékoli chyby nalezené při ověření jsou okamžitě oznámeny uživateli chybovými zprávami.

Diagnóza problému začíná interpretací těchto chybových zpráv a provádí nápravnou akci.

Zpracování problémů

Problémy nalezené během normálního provozu kanálů jsou oznámeny do systémové konzoly nebo do systémového protokolu. Diagnóza problému začíná sběrem všech relevantních informací z protokolu a pokračuje analýzou, aby identifikoval problém.

Potvrzovací a chybové zprávy se vrací do terminálu, který inicioval příkazy, je-li to možné.

Produkt IBM MQ vytváří evidenční a statistické údaje, které lze použít k identifikaci trendů v oblasti využití a výkonu. V systému z/OSse tyto informace vytvářejí ve formě záznamů SMF, podrobnosti naleznete v tématu [Monitorování výkonu a využití prostředků](#). Ekvivalentní informace o jiných platformách jsou vytvářeny jako záznamy PCF, podrobnosti viz [Datové typy Structure](#).

Zprávy a kódy

Informace o zprávách a kódech, které vám pomohou s primární diagnózou problému, najdete v tématu [Zprávy a kódy příčin](#).

Bezpečnost zpráv

Kromě typických funkcí zotavení produktu IBM MQzajišťuje distribuovaná správa front, že zprávy jsou řádně doručovány pomocí procedury synchronizačního bodu koordinované mezi dvěma konci kanálu zpráv. Pokud tento postup zjistí chybu, zavře kanál tak, abyste mohli problém vyšetřit a bezpečně uchovávat zprávy v přenosové frontě, dokud nebude kanál restartován.

Procedura synchronizačního bodu má výhodu, že se pokusí o zotavení situace v *nejistém stavu* při spuštění kanálu. (*Nejisté* je stav jednotky zotavení, pro kterou byl požadován synchronizační bod, ale výsledek požadavku není dosud znám.) Také přidružené k tomuto zařízení jsou tyto dvě funkce:

1. Vyřešit s potvrzením nebo vyřazením
2. Vynulovat pořadové číslo

Použití těchto funkcí probíhá pouze ve výjimečných případech, protože kanál se automaticky obnovuje ve většině případů.

Rychlé, přechodné zprávy

Atribut kanálu přechodných zpráv (NPMSPEED) lze použít k určení, že jakékoli přechodné zprávy na kanálu mají být dodány rychleji. Další informace o tomto atributu najdete v tématu [Nedodržovaná rychlost zpráv \(NPMSPEED\)](#).

Pokud se kanál ukončí během rychlého, netrvalé zprávy jsou v režimu přenosu, zprávy mohou být ztraceny a je na aplikaci, aby bylo možné provést jejich obnovu, je-li to nutné.

Pokud přijímající kanál nemůže vložit zprávu do své cílové fronty, pak je umístěn do fronty nedoručených zpráv, pokud byla definována. Pokud ne, zpráva se vyřadí.

Poznámka: Pokud druhý konec kanálu tuto volbu nepodporuje, kanál se spustí s normální rychlostí.

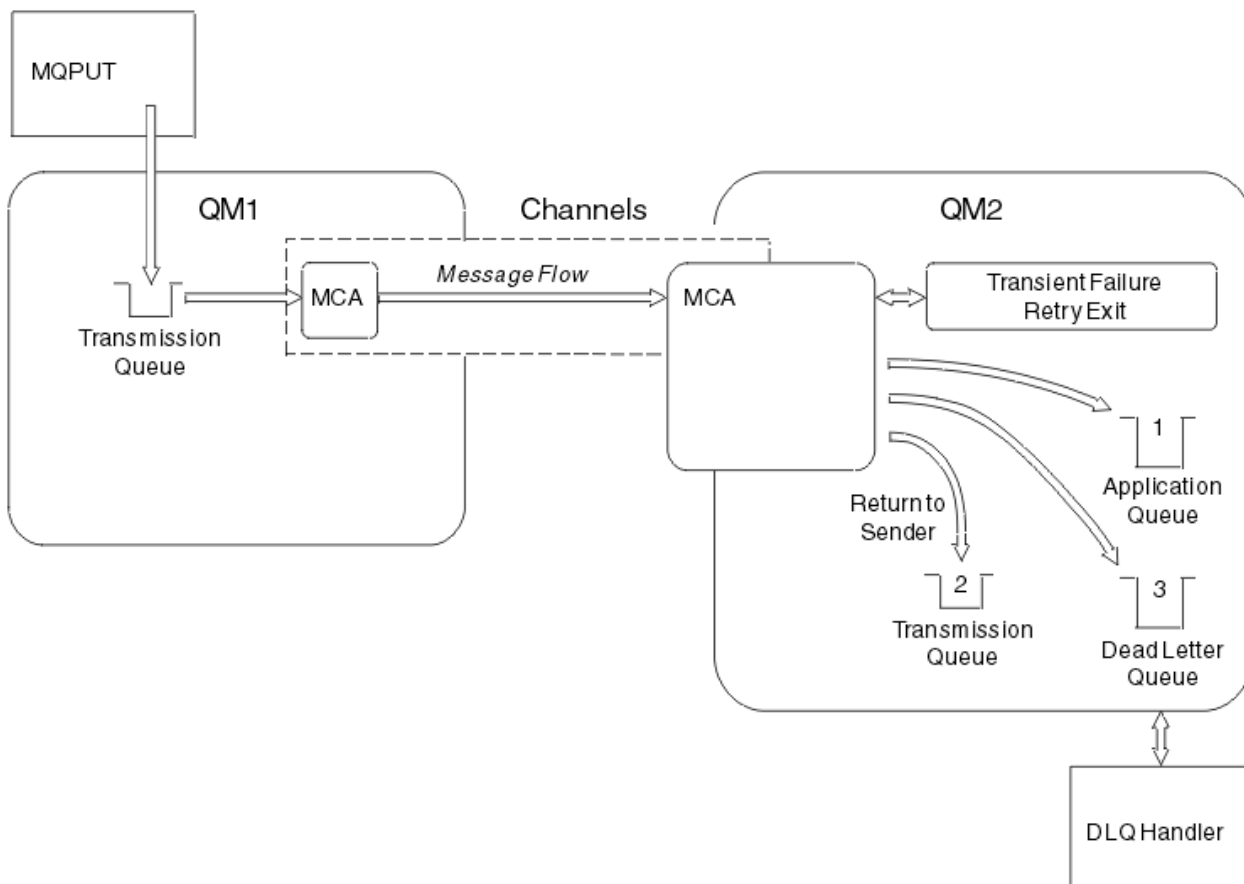
Nedoručené zprávy

Další informace o tom, co se stane, když nelze doručit zprávu, najdete v tématu [“Co se stane, když nebude možné zprávu doručit?”](#) na stránce 165.

Co se stane, když nebude možné zprávu doručit?

Nelze-li zprávu doručit, může ji agent MCA zpracovat několika způsoby. Může to zkusit znovu, může vrátit odesílateli, nebo to může dát do fronty nedoručených zpráv.

Obrázek 23 na stránce 165 uvádí zpracování, které se vyskytne, když agent MCA nemůže vložit zprávu do cílové fronty. (Zobrazené volby se nepoužijí na všechny platformy.)



Obrázek 23. Co se stane, když nelze doručit zprávu

Jak je zobrazeno na obrázku, agent MCA může provádět několik věcí se zprávou, kterou nemůže doručit. Tato akce je určena volbami zadanými při definování kanálu a voleb sestavy MQPUT pro danou zprávu.

1. opakování zprávy

Pokud nemůže agent MCA zařadit do cílové fronty zprávu z příčiny, která by mohla být přechodná (například proto, že je fronta plná), může agent MCA počkat a později zkusit operaci zopakovat. Můžete určit, zda agent MCA čeká, na jak dlouho a kolikrát se to pokusí.

- Při definování kanálu můžete zadat čas opakování zprávy a interval pro chyby MQPUT. Pokud zprávu nelze vložit do cílové fronty, protože je fronta plná nebo je pro vkládání zablokována, program MCA se pokusí o počet zadaných časů v zadaném časovém intervalu.
- Můžete napsat vlastní uživatelskou proceduru pro opakování zpráv. Uživatelská procedura vám umožňuje určit, za jakých podmínek chcete agenta MCA pokusit o zopakování operace MQPUT nebo MQOPEN. Určete název uživatelské procedury při definování kanálu.

2. vrátit odesílateli

Pokud došlo k neúspěšnému pokusu o zopakování zprávy nebo byl zjištěn jiný typ chyby, může agent MCA odeslat zprávu zpět odesílateli. Chcete-li povolit vrácení odesílateli, je třeba při vkládání zprávy do původní fronty určit následující volby v deskriptoru zprávy:

- Volba sestavy MQRO_EXCEPTION_WITH__FULL_DATA
- Volba sestavy MQRO_DISCARD_MSG
- Název fronty pro odpovědi a správce front pro odpovědi.

Pokud program MCA nemůže vložit zprávu do cílové fronty, vygeneruje zprávu o výjimce obsahující původní zprávu a vloží ji do přenosové fronty, která má být odeslána do fronty pro odpovědi určené v původní zprávě. (Je-li fronta pro odpovědi ve stejném správcí front jako MCA, zpráva se umístí přímo do této fronty, nikoli do přenosové fronty.)

3. Fronta nedoručených zpráv

Pokud nelze zprávu doručit nebo vrátit, bude vložena do fronty nedoručených zpráv (DLQ). Obslužnou rutinu DLQ můžete použít ke zpracování zprávy. Toto zpracování je popsáno v tématu [Zpracovávání zpráv ve frontě nedoručených zpráv](#) pro systémy IBM MQ for UNIX, Linux a Windows a v [Obslužném programu obslužné rutiny fronty nedoručených zpráv \(CSQUDLQH\)](#) pro systémy z/OS. Není-li fronta nedoručených zpráv k dispozici, odesílající agent MCA ponechá zprávu v přenosové frontě a kanál se zastaví. Na rychlém kanálu jsou přechodné zprávy, které nelze zapsat do fronty nedoručených zpráv, ztraceny.

Pokud v systému IBM WebSphere MQ 7.0 není definována žádná lokální fronta nedoručených zpráv, vzdálená fronta není k dispozici nebo je definována a neexistuje žádná vzdálená fronta nedoručených zpráv, kanál odesílatele přejde do fronty RETRY a zprávy jsou automaticky odvolány do přenosové fronty.

Související informace



[Použití fronty nedoručených zpráv \(USEDLQ\)](#)

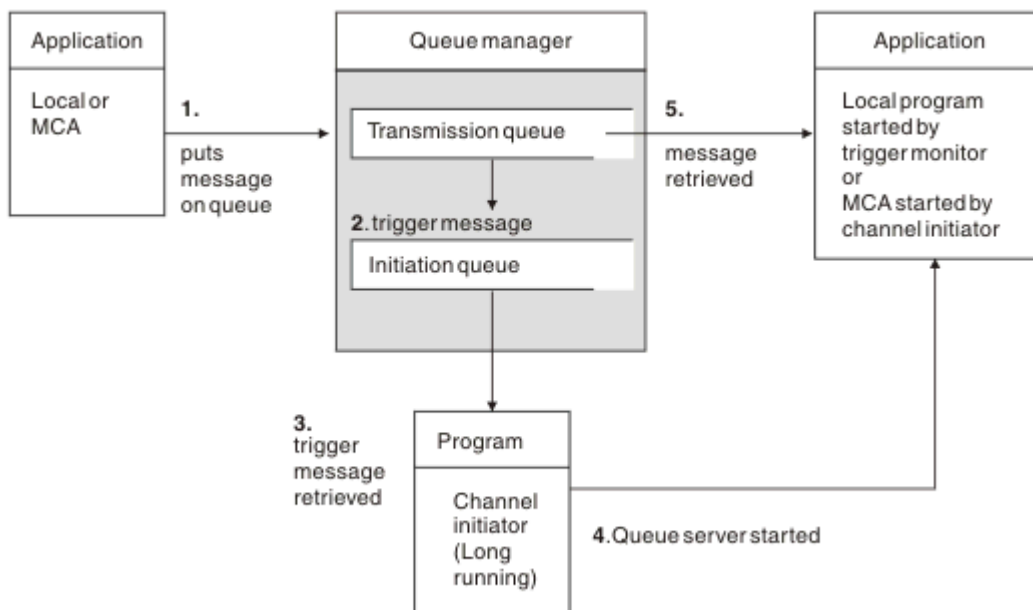
Spouštěcí kanály

Produkt IBM MQ poskytuje službu pro automatické spouštění aplikace, jsou-li splněny určité podmínky ve frontě. Toto zařízení se nazývá spouštění.

Toto vysvětlení je zamýšleno jako přehled spouštěcích koncepcí. Úplný popis naleznete v tématu [Spuštění aplikací produktu IBM MQ pomocí spouštěčů](#).

Informace specifické pro danou platformu naleznete v následujících tématech:

- Pro produkt Windowsviz systémy SYSTÉM UNIX a Linux , [“Spouštění kanálů v systémech UNIX, Linux a Windows .”](#) na stránce 168
-  Pro IBM i viz [“Spouštění kanálů v produktu IBM MQ for IBM i”](#) na stránce 168
-  Pro z/OSviz [“Přenosové fronty a spouštěcí kanály”](#) na stránce 593



Obrázek 24. Koncepty spouštění

Objekty požadované pro spuštění jsou zobrazeny v [Obrázek 24 na stránce 167](#). Zobrazuje následující posloupnost událostí:

1. Lokální správce front umístí zprávu z aplikace nebo z agenta kanálu zpráv (MCA) v přenosové frontě.
2. Když jsou splněny spouštěcí podmínky, umístí lokální správce front zprávu spouštěče do inicializační fronty.
3. Inicializátor kanálu s dlouhou dobou zpracování monitoruje inicializační frontu a načítá zprávy tak, jak přicházejí.
4. Inicializátor kanálu zpracovává zprávy spouštěče podle informací obsažených v těchto zprávách. Tato informace může zahrnovat název kanálu, v tomto případě je spuštěna odpovídající agent MCA.
5. Lokální aplikace nebo agent MCA, který byl spuštěn, načítá zprávy z přenosové fronty.

Chcete-li nastavit tento scénář, musíte:

- Vytvořte přenosovou frontu s názvem inicializační fronty (to znamená SYSTEM.CHANNEL.INITQ) v odpovídajícím atributu.
- Ujistěte se, že je inicializační fronta (SYSTEM.CHANNEL.INITQ) existuje.
- Ujistěte se, že program inicializátoru kanálu je k dispozici a že je spuštěn. Program inicializátoru kanálu musí být zadán spolu s názvem inicializační fronty ve svém počátečním příkazu. **z/OS** V systému z/OS je název inicializační fronty opraven, takže není použit v příkazu ke spuštění.
- Volitelně vytvořte definici procesu pro spuštění, pokud neexistuje, a ujistěte se, že pole *UserData* obsahuje název kanálu, který obsluhuje. Místo vytvoření definice procesu můžete zadat název kanálu v atributu *TriggerData* přenosové fronty. IBM MQ pro systémy **IBM i** IBM i, UNIX, Linux a Windows, umožňují, aby byl název kanálu zadán jako prázdný. V takovém případě se použije první dostupná definice kanálu s touto přenosovou frontou.
- Ujistěte se, že definice přenosové fronty obsahuje název definice procesu, která má sloužit, (je-li to vhodné), jméno inicializační fronty a spouštěcí charakteristiky, které cítíte nejvíce vhodné. Řídící atribut spouštěče umožňuje aktivaci spouštěče, nebo nemusí být, jak je nezbytné.

Poznámka:

1. Inicializátor kanálu pracuje jako monitorování 'spouštěče monitoru', který monitoruje inicializační frontu používanou ke spuštění kanálů.
2. Inicializační fronta a spouštěcí proces lze použít ke spuštění libovolného počtu kanálů.
3. Může být definován libovolný počet inicializačních front a procesů spouštěče.
4. Doporučuje se typ spouštěče FIRST, aby se zabránilo zahlcení systému s inicializačním kanálem.

Spouštění kanálů v systémech UNIX, Linux a Windows .

Můžete vytvořit definici procesu v produktu IBM MQ, definování procesů, které mají být spuštěny. Příkaz MQSC DEFINE PROCESS použijte k vytvoření definice procesu pojmenovává proces, který má být spuštěn při příchodu zpráv do přenosové fronty. Atribut USERDATA definice procesu obsahuje název kanálu, který je obsluhován přenosovou frontou.

Definujte lokální frontu (QM4), která uvádí, že zprávy triggeru se mají zapsat do inicializační fronty (IQ), aby se spustila aplikace, která spouští kanál (QM3.TO.QM4):

```
DEFINE QLOCAL(QM4) TRIGGER INITQ(SYSTEM.CHANNEL.INITQ) PROCESS(P1) USAGE(XMITQ)
```

Definujte aplikaci (proces P1), která má být spuštěna:

```
DEFINE PROCESS(P1) USERDATA(QM3.TO.QM4)
```

Případně u systémů IBM MQ for UNIX, Linux a Windows můžete eliminovat potřebu definice procesu zadáním názvu kanálu v atributu TRIGDATA přenosové fronty.

Definujte lokální frontu (QM4). Určete, že zprávy spouštěče mají být zapsány do výchozí inicializační fronty SYSTEM.CHANNEL.INITQ, chcete-li spustit aplikaci (proces P1), která spouští kanál (QM3.TO.QM4):

```
DEFINE QLOCAL(QM4) TRIGGER INITQ(SYSTEM.CHANNEL.INITQ)
USAGE(XMITQ) TRIGDATA(QM3.TO.QM4)
```

Pokud nezádáte název kanálu, bude inicializátor kanálu hledat v souborech definice kanálu, dokud nenajde kanál, který je přidružen k uvedené přenosové frontě.

Spouštění kanálů v produktu IBM MQ for IBM i

IBM i

Spouštění kanálů v produktu IBM MQ for IBM i je implementováno s procesem inicializátoru kanálu. Proces inicializátoru kanálu pro inicializační frontu SYSTEM.CHANNEL.INITQ se spustí automaticky se správcem front, pokud není zakázán změnou atributu SCHINIT správce front.

Nastavte přenosovou frontu pro kanál tak, že uvedete SYSTEM.CHANNEL.INITQ jako inicializační frontu a povolení spuštění pro frontu. Inicializátor kanálu spustí první dostupný kanál, který uvádí tuto přenosovou frontu.

```
CRTMQMQ QNAME(MYXMITQ1) QTYPE(*LCL) MQMNAME(MYQMGR)
TRGENBL(*YES) INITQNAME(SYSTEM.CHANNEL.INITQ)
USAGE(*TMQ)
```

Můžete manuálně spustit až tři procesy inicializátoru kanálu s příkazem STRMQMCHLI a uvést různé inicializační fronty. Můžete také zadat více než jeden kanál, který dokáže zpracovat přenosovou frontu, a zvolit, který kanál se má spustit. Tato schopnost je stále poskytována jako kompatibilní se staršími verzemi. Jeho použití je zamítnuté.

Poznámka: Pouze jeden kanál v daném okamžiku může zpracovávat přenosovou frontu.

```
STRMQMCHLI QNAME(MYINITQ)
```

Nastavte přenosovou frontu pro kanál zadáním parametru TRGENBL (*YES) a výběrem kanálu, který se má pokusit o spuštění, určete název kanálu v poli TRIGDATA. Příklad:

```
CRTMQMQ QNAME(MYXMITQ2) QTYPE(*LCL) MQMNAME(MYQMGR)  
TRGENBL(*YES) INITQNAME(MYINITQ)  
USAGE(*TMQ) TRIGDATA(MYCHANNEL)
```

Související pojmy

[“Spuštění a zastavení inicializátoru kanálu” na stránce 169](#)

Spouštěcí impuls je implementován pomocí procesu inicializátoru kanálu.

[“Konfigurace distribuovaných front” na stránce 124](#)

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ, včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související informace

[Kanálové programy v systémech SYSTÉM UNIX, Linuxa Okna](#)

 [Interkomunikační úlohy v systému IBM i](#)

 [Stav kanálů v systému IBM i](#)

Spuštění a zastavení inicializátoru kanálu


Spouštěcí impuls je implementován pomocí procesu inicializátoru kanálu.

Tento proces inicializátoru kanálu je spuštěn s příkazem MQSC START CHINIT. Pokud nepoužíváte výchozí inicializační frontu, zadejte do příkazu název inicializační fronty. Chcete-li například použít příkaz START CHINIT ke spuštění fronty IQ pro výchozího správce front, zadejte:

```
START CHINIT INITQ(IQ)
```

Ve výchozím nastavení je inicializátor kanálu spuštěn automaticky s použitím výchozí inicializační fronty SYSTEM.CHANNEL.INITQ. Chcete-li spustit všechny inicializátory kanálu ručně, postupujte takto:

1. Vytvořte a spusťte správce front.
2. Změnit vlastnost SCHINIT správce front na hodnotu MANUAL.
3. Ukončete a znovu spusťte správce front.

V systémech  IBM MQ for iSeries, UNIX, Linux a Windows se inicializátor kanálu spouští automaticky. Počet inicializátorů kanálu, které lze spustit, je omezen. Výchozí a současně maximální hodnota je 3. Tuto hodnotu můžete změnit pomocí parametru MAXINITIATORS v souboru qm.ini pro systémy SYSTÉM UNIX a Linux a v registru pro systémy Windows .

Podrobnosti o příkazu spuštění inicializátoru kanálu **runmqchla** o dalších řídicích příkazech najdete v tématu [Řídicí příkazy produktu IBM MQ](#) .

Zastavení inicializátoru kanálu

Výchozí inicializátor kanálu je spuštěn automaticky při spuštění správce front. Všechny inicializátory kanálu jsou automaticky zastaveny, pokud je správce front zastaven.

Inicializační a konfigurační soubory

Způsob zpracování inicializačních dat kanálu závisí na platformě IBM MQ .

z/OS systémy

z/OS

V produktu IBM MQ for z/OS jsou informace o inicializaci a konfiguraci zadány pomocí příkazu ALTER QMGR MQSC. Pokud do vstupní datové sady inicializace CSQINP2 vložíte příkazy ALTER QMGR, budou tyto příkazy zpracovány při každém spuštění správce front.

Chcete-li spustit příkazy MQSC, jako např. START LISTENER při každém spuštění inicializátoru kanálu, vložte je do vstupní datové sady inicializace CSQINPX a zadejte do procedury spuštění úlohy iniciátoru kanálu nepovinný příkaz DD CSQINPX.


Další informace o systémech CSQINP2 a CSQINPX naleznete v tématu [Úprava vstupních datových sad inicializace ALTER QMGR](#).

Systémy Windows, IBM i, SYSTÉM UNIX a Linux

V systémech IBM MQ for Windows,  IBM i, SYSTÉM UNIX a Linux existují *konfigurační soubory* pro uložení základních konfiguračních informací o instalaci produktu IBM MQ .

Existují dva konfigurační soubory: jedno platí pro daný počítač, druhé platí pro jednotlivého správce front.

IBM MQ konfigurační soubor

Tento soubor obsahuje informace vztahující se ke všem správcům front v systému IBM MQ . Soubor se nazývá `mqs.ini`. Je plně popsán v publikaci [Správa pro IBM MQ for Windows](#),  a v [Administering IBM i](#) , a v systémech SYSTÉM UNIX a Linux .

Konfigurační soubor správce front

Tento soubor obsahuje informace o konfiguraci týkající se jednoho konkrétního správce front. Tento soubor se nazývá `qm.ini`.

Vytvoří se během vytváření správce front a může uchovávat informace o konfiguraci odpovídající libovolnému aspektu správce front. Informace obsažené v souboru obsahují podrobnosti o tom, jak se konfigurace protokolu liší od výchozí konfigurace v konfiguračním souboru IBM MQ .

Konfigurační soubor správce front je umístěn v kořenovém adresáři stromu adresáře obsazeného správcem front. Například pro atributy `DefaultPath` budou konfigurační soubory správce front pro správce front s názvem `QMNAME` vypadat takto:

Pro systémy SYSTÉM UNIX a Linux :

```
/var/mqm/qmgrs/QMNAME/qm.ini
```

Následuje výňatek souboru `qm.ini` . Určuje, že modul listener protokolu TCP/IP má naslouchat na portu 2500, maximální počet aktuálních kanálů má být 200 a maximální počet aktivních kanálů musí být 100.

```
TCP:  
Port=2500  
CHANNELS:  
MaxChannels=200  
MaxActiveChannels=100
```

Můžete zadat rozsah portů TCP/IP, které má být použit pro odchozí kanál. Jednou z metod je použití souboru `qm.ini` k určení začátku a konce rozsahu hodnot portů. Následující příklad ukazuje soubor `qm.ini` s uvedením rozsahu kanálů:

```
TCP:  
StrPort=2500  
EndPort=3000  
CHANNELS:
```

```
MaxChannels=200
MaxActiveChannels=100
```

Uvedete-li hodnotu pro StrPort nebo EndPort , musíte zadat hodnotu pro obě hodnoty. Hodnota parametru EndPort musí být vždy větší než hodnota parametru StrPort.

Kanál se pokusí použít každou z hodnot portů v určeném rozsahu. Když je připojení úspěšné, hodnota portu je port, který kanál poté použije.

 Pro IBM i:

```
/QIBM/UserData/mqm/qmgrs/QMNAME/qm.ini
```

Pro systémy Windows :

```
C:\ProgramData\IBM\MQ\qmgrs\QMNAME\qm.ini
```

Další informace o souborech qm.ini naleznete v tématu [Stanzy konfiguračního souboru pro distribuované ukládání do fronty](#).

Převod dat

Zprávy produktu IBM MQ mohou vyžadovat převod dat při odesílání mezi frontami v různých správcích front.

Zpráva IBM MQ se skládá ze dvou částí:

- Řízení informací v deskriptoru zpráv
- Data aplikace

Obě části mohou vyžadovat konverzi dat, jsou-li odeslány mezi frontami v různých správcích front. Další informace o převodu dat aplikací naleznete v tématu [Převod dat aplikací](#).

Psaní vlastních agentů kanálů zpráv

IBM MQ vám umožňuje zapsat si vlastní programy MCA (Message Channel Agent) nebo instalovat jeden z nezávislých dodavatelů softwaru.

Je možné, že budete chtít napsat své vlastní programy MCA, aby produkt IBM MQ pracoval nad vaším vlastním interním komunikačním protokolem nebo aby odesílal zprávy prostřednictvím protokolu, který produkt IBM MQ nepodporuje. (Chcete-li spolupracovat s agentem MCA pro práci s produktem IBM MQ na druhém konci, nelze zapsat vlastní program MCA.)

Pokud se rozhodnete použít agenta MCA, který nebyl dodán produktem IBM MQ, je třeba vzít v úvahu následující body.

Odeslání a příjem zprávy

Musíte napsat odesílající aplikaci, která bude přijímat zprávy z místa, kde je aplikace uvede, například z přenosové fronty, a odešle je na protokol, se kterým chcete komunikovat. Musíte také napsat přijímající aplikaci, která přijímá zprávy z tohoto protokolu a vkládá je do cílových front. Odesílající a přijímající aplikace používají volání rozhraní fronty zpráv (MQI), nikoli žádná speciální rozhraní.

Musíte zajistit, aby zprávy byly doručeny pouze jednou. Koordinace bodů synchronizace může být použita k pomoci s tímto doručením.

Řídící funkce kanálu

Chcete-li řídit kanály, musíte zadat své vlastní administrativní funkce. Administrační funkce kanálu produktu IBM MQ nelze použít pro konfiguraci (například příkaz DEFINE CHANNEL) nebo pro monitorování (například DISPLAY CHSTATUS) kanály.

Inicializační soubor

Pokud vyžadujete vlastní inicializační soubor, musíte zadat vlastní soubor inicializace.

Převod dat aplikace

Pravděpodobně budete chtít povolit konverzi dat pro zprávy, které posíláte do jiného systému. Je-li tomu tak, použijte volbu MQGMO_CONVERT při volání MQGET při načítání zpráv z libovolného místa, kde je aplikace umístuje, například k přenosové frontě.

Uživatelské procedury

Zvažte, zda nepotřebujete uživatelské procedury. Pokud ano, můžete použít stejné definice rozhraní, které produkt IBM MQ používá.

Spouštění

Pokud vaše aplikace umísťuje zprávy do přenosové fronty, můžete nastavit atributy přenosové fronty tak, aby odesílaná MCA byla spuštěna, když zprávy dorazí do fronty.


Inicializátor kanálu

Je možné, že budete muset zadat svůj vlastní iniciátor kanálu.

Další informace, které je třeba zvážit při správě distribuovaných front

Další témata, která je třeba zvážit při přípravě produktu IBM MQ pro distribuovanou správu front. Toto téma pokrývá frontu nedoručených zpráv, Fronty v použití, Rozšíření systému a programy uživatelských procedur a Spouštění kanálů a listenerů jako ověřené aplikace.


Nedoručená-fronta zpráv

Chcete-li zajistit, aby byly zpracovány zprávy přicházející do fronty nedoručených zpráv (známé také jako fronta nedoručených zpráv nebo DLQ), vytvořte program, který lze spustit nebo spustit v pravidelných intervalech pro zpracování těchto zpráv. Obslužná rutina DLQ je poskytována s produktem IBM MQ v systémech SYSTÉM UNIX a Linux . Další informace najdete v tématu [Ukázka obslužné rutiny DLQ, amqsdlq.](#)  Další informace o příkazu IBM MQ for IBM inaleznete v tématu [Obslužná rutina fronty nedoručených zpráv produktu IBM MQ for IBM i.](#)

Fronty se používají

MCAs pro přijímací kanály může udržet cílové fronty otevřené i v případě, že zprávy nejsou přenášeny. Tyto výsledky ve frontách se zobrazují jako "v použití".

Maximální počet kanálů

 V IBM MQ for IBM i můžete uvést maximální počet kanálů povolených ve vašem systému a maximální počet kanálů, které mohou být aktivní najednou. Tato čísla uvedete v souboru qm.ini v adresáři QIBM/UserData/mqm/qmgrs/queue_manager_name. Viz [Stanzy konfiguračního souboru pro distribuované ukládání do fronty.](#)

Rozšíření systému a programy uživatelské procedury

V definici kanálu je k dispozici zařízení, které umožňuje spouštění dalších programů v definovaných časech během zpracování zpráv. Tyto programy nejsou dodávány s produktem IBM MQ, ale lze je poskytovat každou instalaci v souladu s místními požadavky.

Mají-li být tyto uživatelské programy spuštěny, musí mít předem definované názvy a musí být dostupné pro volání programů kanálu. Názvy programů uživatelských procedur jsou obsaženy v definicích kanálů zpráv.

Existuje definované řídicí blokovací rozhraní pro předání řízení těmto programům a pro manipulaci s návratem řízení z těchto programů.

Přesná místa, kde jsou tyto programy volány, a podrobnosti o řídicích blocích a názvech, najdete v tématu [Programy výstupních bodů kanálů pro kanály systému zpráv.](#)

Spuštění kanálů a listenerů jako důvěryhodných aplikací

Je-li výkon důležitým aspektem ve vašem prostředí a vaše prostředí je stabilní, můžete kanály a moduly listener spouštět jako důvěryhodné s použitím vazby FASTPATH. Existují dva faktory, které ovlivňují, zda jsou kanály a listenery spuštěny jako důvěryhodné:

- Proměnná prostředí MQ_CONNECT_TYPE=FASTPATH nebo MQ_CONNECT_TYPE = STANDARD. Rozlišují se malá a velká písmena. Uvedete-li hodnotu, která není platná, je ignorována.
- MQIBindType ve stanze Channels v souboru qm . ini nebo v souboru registru. Můžete jej nastavit na hodnotu FASTPATH nebo STANDARD a nerozlišují se malá a velká písmena. Výchozí hodnota je STANDARD.

Parametr MQIBindType můžete použít ve spojení s proměnnou prostředí k dosažení požadovaného účinku následujícím způsobem:

MQIBindType	Proměnná prostředí	Výsledek
STANDARD	Nedefinovaný	STANDARD
Rychlý	Nedefinovaný	Rychlý
STANDARD	STANDARD	STANDARD
Rychlý	STANDARD	STANDARD
STANDARD	Rychlý	STANDARD
Rychlý	Rychlý	Rychlý
STANDARD	CLIENT	CLIENT
Rychlý	CLIENT	STANDARD
STANDARD	LOKÁLNÍ	STANDARD
Rychlý	LOKÁLNÍ	STANDARD

V souhrnu existují pouze dva způsoby, jak lze kanály a listenery spustit jako důvěryhodné:

1. Uvedením parametru MQIBindType= FASTPATH v produktu qm . ini nebo v registru a neurčujete proměnnou prostředí.
2. Zadáním parametru MQIBindType= FASTPATH v produktu qm . ini nebo do registru a nastavením proměnné prostředí na hodnotu FASTPATH.

Zvažte spuštění listenerů jako důvěryhodných, protože listenery jsou stabilní procesy. Pokud nepoužíváte nestálý kanál nebo příkaz STOP CHANNEL MODE (TERMINATE), zvažte spuštění kanálů jako důvěryhodnosti.

Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux

Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, aplikací IBM MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro synchronizační informace.

Můžete použít následující typy příkazů:

Příkazy IBM MQ (MQSC)

Prostředí MQSC můžete použít jako jednotlivé příkazy v relaci MQSC v systému Windows, v systémech SYSTÉM UNIX a Linux . Chcete-li vydat více komplikovaných nebo více příkazů, můžete prostředí MQSC sestavit do souboru, který lze poté spustit z příkazového řádku. Další informace najdete v tématu [Příkazy MQSC](#). Tento oddíl uvádí některé jednoduché příklady použití MQSC pro distribuované fronty.

Příkazy kanálu jsou podmnožinou příkazů IBM MQ (MQSC). Použijte MQSC a řídicí příkazy pro:

- Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálu

- Spuštění a zastavení kanálů, testování spojení, resetování pořadových čísel kanálů a řešení sporných zpráv, pokud nelze znovu zavést propojení
- Zobrazení informací o stavu kanálů

Řídící příkazy

Pro některé z těchto funkcí můžete také zadat příkaz *control commands* na příkazovém řádku. Další informace viz [řídící příkazy](#).

Formátovací příkazy Programovatelného příkazu

Podrobnosti naleznete v tématu [Příkazy PCF](#).

IBM MQ Průzkumník

V systémech UNIX, Linux a Windows můžete použít Průzkumníka IBM MQ . To poskytuje grafické rozhraní administrace pro provádění administrativních úloh jako alternativu k použití řídicích příkazů nebo příkazů MQSC. Definice kanálů jsou drženy jako objekty správce front.

Každý správce front má komponentu DQM pro řízení propojení mezi kompatibilními vzdálenými správci front. Oblast úložiště obsahuje pořadová čísla a *logical unit of work (LUW)* identifikátorů. Ty se používají pro účely synchronizace kanálu.

Seznam funkcí, které jsou vám k dispozici při nastavování a řízení kanálů zpráv s použitím různých typů příkazů, viz [Tabulka 20 na stránce 175](#).

Související pojmy

[“Začínáme s objekty” na stránce 176](#)

Kanály musí být definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál. Tento oddíl ukazuje, jak.

[“Nastavení komunikace pro Windows” na stránce 183](#)

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby to uspělo, je nezbytné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak to provést pomocí jedné ze čtyř forem komunikace pro systémy IBM MQ for Windows .

[“Nastavení komunikace v systémech SYSTÉM UNIX a Linux” na stránce 190](#)

DQM je prostředek vzdáleného řazení do fronty pro produkt IBM MQ . Poskytuje řídicí programy kanálu pro správce front, které tvoří rozhraní pro komunikační propojení, ovladatelné systémovým operátorem. Definice kanálů v rámci správy distribuovaných front používají tato připojení.

[“Monitorování a řízení kanálů v systému IBM i” na stránce 195](#)

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

Související informace

[Kanálové programy v systémech SYSTÉM UNIX, Linux a Okna](#)

[Příklad plánování kanálů zpráv pro distribuované platformy](#)

[Příklad konfiguračních informací](#)

[Atributy kanálu](#)

Funkce vyžadované pro nastavení a řízení kanálů

Pro nastavení a řízení kanálů může být zapotřebí řada funkcí IBM MQ . Funkce kanálu jsou vysvětleny v tomto tématu.

Definici kanálu můžete vytvořit s použitím výchozích hodnot dodaných produktem IBM MQa s určením názvu kanálu, typu vytvářeného kanálu, metody komunikace, která má být použita, název přenosové fronty a název připojení.

Název kanálu musí být stejný na obou koncích kanálu a musí být jedinečný v rámci sítě. Musíte však omezit použité znaky na ty znaky, které jsou platné pro názvy objektů produktu IBM MQ .

Informace o dalších funkcích souvisejících s kanálem naleznete v následujících tématech:

- [“Začínáme s objekty” na stránce 176](#)
- [“Vytváření přidružených objektů” na stránce 177](#)

- [“Vytváření výchozích objektů” na stránce 177](#)
- [“Vytvoření kanálu” na stránce 177](#)
- [“Zobrazení kanálu” na stránce 178](#)
- [“Zobrazení stavu kanálu” na stránce 178](#)
- [“Kontrola odkazů pomocí příkazu ping” na stránce 179](#)
- [“Spuštění kanálu” na stránce 179](#)
- [“Zastavení kanálu” na stránce 181](#)
- [“Přejmenování kanálu” na stránce 181](#)
- [“Resetování kanálu” na stránce 182](#)
- [“Vyřešení nejistých zpráv na kanálu” na stránce 182](#)

Produkt Tabulka 20 na stránce 175 zobrazí úplný seznam funkcí produktu IBM MQ , které můžete potřebovat.

<i>Tabulka 20. Funkce požadované v systémech Windows, SYSTÉM UNIX a Linux</i>			
Funkce	Řídící příkazy	MQSC	Ekvivalent průzkumníka IBM MQ ?
Funkce správce front			
Změnit správce front		ALTER QMGR	Ano
Vytvoření správce front	crtmqm		Ano
Odstranit správce front	dlmqm		Ano
Zobrazit správce front		ZOBRAZIT QMGR	Ano
Ukončení správce front	endmqm		Ano
Odeslat signál Ping pro správce front		PING QMGR	Ne
Spustit správce front	strmqm		Ano
Funkce příkazového serveru			
Zobrazit příkazový server	dspmqcsv		Ne
Ukončit příkazový server	endmqcsv		Ne
Spustit příkazový server	strmqcsv		Ne
Funkce fronty			
Změnit frontu		POZMĚNIT PŘÍKAZ QALIAS ALTER QLOCAL ALTER QMODEL ALTER QREMOTE Viz téma Fronty ALTER .	Ano
Vymazat frontu		CLEAR QLOCAL	Ano
Vytvořit frontu		DEFINE QALIAS DEFINE QLOCAL DEFINE QMODEL DEFINE QREMOTE Viz DEFINE queues .	Ano

Tabulka 20. Funkce požadované v systémech Windows, SYSTÉM UNIX a Linux (pokračování)

Funkce	Řídící příkazy	MQSC	Ekvivalent průzkumníka IBM MQ ?
Odstranit frontu		VÝMAZ QALIAS DELETE QLOCAL DELETE QMODEL DELETE QREMOTE Viz <u>DELETE queues</u> .	Ano
Zobrazit frontu		ZOBRAZIT FRONTU	Ano
funkce procesu			
Změnit proces		ZMĚNA PROCES	Ano
Vytvořit proces		DEFINOVAT PROCES	Ano
Odstranit proces		<u>Odstranit proces</u>	Ano
Zobrazit proces		ZOBRAZIT PROCES	Ano
Funkce kanálu			
Změnit kanál		ALTER CHANNEL	Ano
Vytvořit kanál		<u>Definovat kanál</u>	Ano
Odstranit kanál		<u>Odstranit kanál</u>	Ano
Zobrazit kanál		DISPLAY CHANNEL	Ano
Zobrazit stav kanálu		ZOBRAZIT STAV CHSTATUS	Ano
Ukončit kanál		<u>Ukončit kanál</u>	Ano
Odeslat signál Ping pro kanál		<u>Odeslat signál Ping pro kanál</u>	Ano
Resetovat kanál		<u>Resetovat kanál</u>	Ano
Vyřešit kanál		<u>Vyřešit kanál</u>	Ano
Spustit kanál	<u>runmqchl</u>	<u>Spustit kanál</u>	Ano
Spustit inicializátor kanálu	<u>runmqchi</u>	START CHINIT	Ne
Spustit modul listener ¹	<u>runmqlsr</u>	<u>Spustit listener</u>	Ne
Koncový modul listener	<u>endmqlsr</u> (systémy Windows , AIX, HP-UX a Solaris)		Ne

Poznámka:

1. Modul listener může být spuštěn automaticky při spuštění správce front.

Začínáme s objekty

Kanály musí být definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál. Tento oddíl ukazuje, jak.

Pomocí příkazů IBM MQ (MQSC) nebo Průzkumníka IBM MQ postupujte takto:

1. Definování kanálů zpráv a přidružených objektů
2. Monitorování a řízení kanálů zpráv

Je možné, že přidružené objekty, které budete potřebovat definovat, jsou:

- Přenosové fronty
- Definice vzdálených front
- Definice aliasů správce front
- Definice aliasů fronty odpovědi
- Odpovědi na lokální fronty
- Procesy pro spouštění (MCA)
- Definice kanálů zpráv

Před spuštěním kanálu musí být definován a dostupný konkrétní komunikační spoj pro každý kanál. Popis způsobu, jakým jsou definovány propojení LU 6.2, TCP/IP, NetBIOS, SPX a DECnet, najdete v příslušné komunikační příručce pro vaši instalaci. Viz také [Příklad konfiguračních informací](#).

Další informace o vytváření a práci s objekty naleznete v následujících dílčích tématech:

Vytváření přidružených objektů

Prostředí MQSC se používá k vytvoření přidružených objektů.

Pomocí MQSC vytvořte frontu a objekty aliasu: přenosové fronty, definice vzdálených front, definice aliasů správce front, definice alias fronty odpovědi a odpovědi na lokální fronty.

Rovněž vytvořte definice procesů pro spouštění (MCAs) podobným způsobem.

Příklad, jak vytvořit všechny požadované objekty, najdete v tématu [Příklad plánování kanálů zpráv pro distribuované platformy](#).

Vytváření výchozích objektů

Výchozí objekty jsou vytvářeny automaticky při vytvoření správce front. Těmito objekty jsou fronty, kanály, definice procesu a fronty administrace. Jakmile jsou výchozí objekty vytvořeny, můžete je kdykoli nahradit spuštěním příkazu `strmqm` s volbou `-c`.

Použijete-li příkaz `crtmqm` k vytvoření správce front, příkaz také inicializuje program a vytvoří sadu výchozích objektů.

1. Každý výchozí objekt je vytvořen na oplátku. Program uchovává počet úspěšně definovaných objektů, počet existujících objektů a jejich nahrazení a počet neúspěšných pokusů o jejich provedení.
2. Program zobrazí výsledky pro vás, a pokud došlo k nějakým chybám, přesměrovává vás do příslušného protokolu chyb kvůli podrobnostem.

Po dokončení spuštění programu můžete pomocí příkazu `strmqm` spustit správce front.

Další informace o příkazech `crtmqm` a `strmqm` najdete v tématu [Řídící příkazy](#).

Změna výchozích objektů

Pokud zadáte volbu `-c`, správce front bude během vytváření objektů spuštěn dočasně a poté se znovu vypne. Při vydání příkazu `strmqm` s volbou `-c` se obnoví existující systémové objekty s výchozími hodnotami (například atribut `MCAUSER` definice kanálu je nastaven na prázdné). Chcete-li spustit správce front, je třeba příkaz `strmqm` znovu použít bez volby `-c`.

Chcete-li změnit výchozí objekty, můžete vytvořit svou vlastní verzi starého souboru `amqscoma.tst` a upravit ji.

Vytvoření kanálu

Vytvořte **dvě** definice kanálu, jeden na každém konci připojení. První definici kanálu vytvořte v prvním správci front. Poté vytvořte druhou definici kanálu v druhém správci front na druhém konci odkazu.

Oba konce musí být definovány pomocí názvu kanálu **stejný** . Dva konce musí mít **kompatibilní** typy kanálů, například: Odesílatel a Příjemce.

Chcete-li vytvořit definici kanálu pro jeden konec odkazu, použijte příkaz MQSC DEFINE CHANNEL. Zahrňte název kanálu, typ kanálu pro tento konec připojení, název připojení, popis (je-li požadován), název přenosové fronty (je-li to požadováno) a přenosový protokol. Zahrňte také všechny ostatní atributy, které se mají lišit od výchozích hodnot systému pro požadovaný typ kanálu, pomocí informací, které jste shromáždili dříve.

Poskytli jste nápovědu při rozhodování o hodnotách atributů kanálu v části [Atributy kanálu](#).

Poznámka: Doporučuje se, abyste všechny kanály ve vaší síti pojmenovali jedinečně. Začlenění názvů zdrojového a cílového správce front do názvu kanálu je dobrý způsob, jak to provést.

Příklad příkazu create channel

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) +  
DESCR('Sender channel to QM2') +  
CONNNAME(QM2) TRPTYPE(TCP) XMITQ(QM2) CONVERT(YES)
```

Ve všech příkladech příkazu MQSC se příkaz zobrazí tak, jak se objevuje v souboru příkazů, a jak je napsáno v systémech Windows nebo UNIX nebo Linux . Tyto dvě metody vypadají stejně, kromě toho, že chcete-li spustit příkaz interaktivně, musíte nejprve spustit relaci MQSC. Zadejte `runmqsc`, pro výchozího správce front nebo `runmqsc qmname`, kde `qmname` je název požadovaného správce front. Pak zadejte libovolný počet příkazů, jak je uvedeno v příkladech.

Pro přenositelnost omezte délku řádku svých příkazů na 72 znaků. Použijte znak zřetězení, + , jak je zobrazeno pro pokračování více než jednoho řádku. V systému Windows použijte klávesu Ctrl-z k ukončení položky na příkazovém řádku. V systémech SYSTÉM UNIX a Linux použijte klávesu Ctrl-d. Případně, v systémech UNIX, Linux nebo Windows použijte příkaz **end** .

Zobrazení kanálu

Chcete-li zobrazit atributy kanálu, použijte příkaz MQSC DISPLAY CHANNEL.

Parametr ALL příkazu DISPLAY CHANNEL se standardně předpokládá, pokud nejsou požadovány žádné specifické atributy a uvedený název kanálu není generický.

Atributy jsou popsány v části [Atributy kanálu](#).

Zobrazit příklady kanálů

```
DISPLAY CHANNEL(QM1.TO.QM2) TRPTYPE,CONVERT  
DISPLAY CHANNEL(QM1.TO.*) TRPTYPE,CONVERT  
DISPLAY CHANNEL(*) TRPTYPE,CONVERT  
DISPLAY CHANNEL(QM1.TO.QMR34) ALL
```

Zobrazení stavu kanálu

Použijte příkaz MQSC DISPLAY CHSTATUS uvedením názvu kanálu a toho, zda chcete aktuální stav kanálů nebo stav uložených informací.

ZOBRAZIT CHSTATUS se vztahuje na všechny kanály zpráv. Nevztahuje se na kanály MQI jiné než kanály připojení serveru.

Zobrazené informace zahrnují:

- Název kanálu
- Název komunikačního připojení
- Na nejistém stavu kanálu (je-li to vhodné)

- Poslední pořadové číslo
- Název přenosové fronty (je-li to vhodné)
- Identifikátor v nejistém stavu (je-li to vhodné)
- Poslední potvrzené pořadové číslo
- Identifikátor logické pracovní jednotky
- ID procesu
- ID vlákna (pouze Windows)

Zobrazit příklady stavu kanálu

```
DISPLAY CHSTATUS(*) CURRENT
DISPLAY CHSTATUS(QM1.TO.*) SAVED
```

Uložený stav se neuplatní, dokud nebude na kanálu přenesena alespoň jedna dávka zpráv. Stav se také uloží, když je kanál zastaven (pomocí příkazu STOP CHL) a když je ukončen správce front.

Kontrola odkazů pomocí příkazu ping

Použijte příkaz MQSC pro příkaz PING CHANNEL, chcete-li vyměnit zprávu s pevnou datovou zprávou se vzdáleným koncem.

Příkaz Ping poskytuje určitou jistotu supervizorovi systému, že je tento odkaz k dispozici a funkční.

Příkaz ping nezahrnuje použití přenosových front a cílových front. Používá definice kanálu, související komunikační linku a nastavení sítě. Lze ji použít pouze v případě, že kanál není momentálně aktivní.

Je k dispozici pouze pro kanály odesílatele, serveru a odesílatele klastru. Odpovídající kanál se spouští na vzdálené straně odkazu a provádí vyjednávání parametrů spuštění. Chyby jsou oznámeny normálně.

Výsledek výměny zpráv se zobrazí jako Ping complete nebo chybová zpráva.

Příkaz ping s LU 6.2

Je-li příkaz PING vyvolán, standardně se do přijímacího konce nepřenášejí žádné ID uživatele nebo heslo. Jsou-li požadovány ID uživatele a heslo, mohou být vytvořeny na začátku inicializace v definici kanálu. Je-li heslo zadáno do definice kanálu, je před uložením zašifrováno produktem IBM MQ . Je poté dešifrováno před proudícím konverzací v rámci konverzace.

Spuštění kanálu

Použijte příkaz MQSC START CHANNEL pro kanály odesílatele, serveru a žadatele. Aby aplikace mohly vyměňovat zprávy, musíte spustit program listener pro příchozí připojení.

Příkaz START CHANNEL není nutný, pokud byl kanál nastaven s použitím spouštěče správce front.

Když je spuštěna, odesílající agent MCA přečte definice kanálu a otevře přenosovou frontu. Je vydána spouštěcí posloupnost kanálu, která vzdáleně spustí odpovídající MCA přijímače nebo kanálu serveru. Po spuštění budou procesy odesílatele a serveru čekat na zprávy přicházející do přenosové fronty a předávají je, jakmile dorazí.

Používáte-li spouštěcí nebo spouštěcí kanály jako podprocesy, ujistěte se, že je k dispozici inicializátor kanálu pro monitorování inicializační fronty. Inicializátor kanálu je standardně spuštěn jako součást správce front.

Avšak TCP a LU 6.2 poskytují další schopnosti:

- Pro protokol TCP na systémech SYSTÉM UNIX a Linux může být démon inetd konfigurován pro spuštění kanálu. inetd se spouští jako oddělený proces.

- Pro LU 6.2 v systémech SYSTÉM UNIX a Linux nakonfigurujte svůj produkt SNA tak, aby spustil proces odpovídajícího modulu LU 6.2 .
- Pro LU 6.2 v systémech Windows pomocí serveru SNA můžete použít program TpStart (obslužný program dodávaný se serverem SNA) ke spuštění kanálu. TpStart se spustí jako oddělený proces.

Použití volby Start vždy způsobí, že se kanál resynchronizuje, je-li to nutné.

Aby bylo možné začít úspěšně:

- Definice kanálů, lokální a vzdálené, musí existovat. Pokud neexistuje vhodná definice kanálu pro přijímací kanál nebo kanál připojení serveru, vytvoří se automaticky, je-li kanál automaticky definován, automaticky. Viz [Channel auto-definition exit program](#).
- Přenosová fronta musí existovat a nesmí ji používat žádné jiné kanály.
- MCAs, místní a vzdálený, musí existovat.
- Komunikační spojení musí být k dispozici.
- Správci front musí být spuštěni, lokálními a vzdálenými.
- Kanál zpráv nesmí být již spuštěn.

Zobrazí se zpráva potvrzující, že požadavek na spuštění kanálu byl přijat. Pro potvrzení, že spouštěcí příkaz byl úspěšný, zkontrolujte záznam chyb nebo použijte DISPLAY CHSTATUS. Protokoly chyb jsou:

Windows

`MQ_INSTALLATION_PATH\qmgrs\qmname\errors\AMQERR01 . LOG` (pro každého správce front s názvem qmname)

`MQ_INSTALLATION_PATH\qmgrs\@SYSTEM\errors\AMQERR01 . LOG` (pro obecné chyby)

`MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

Poznámka: V systému Windows se stále také zobrazí zpráva v protokolu událostí aplikace systému Windows .

Systémy SYSTÉM UNIX a Linux

`/var/mqm/qmgrs/qmname/errors/AMQERR01 . LOG` (pro každého správce front s názvem qmname)

`/var/mqm/qmgrs/@SYSTEM/errors/AMQERR01 . LOG` (pro obecné chyby)

Na systémech Windows, SYSTÉM UNIX a Linux použijte příkaz `runmqclsr` ke spuštění procesu modulu listener produktu IBM MQ . Při výchozím nastavení všechny příchozí požadavky na připojení kanálu způsobí spuštění modulu listener MCA jako podprocesy procesu `amqrmppa`.

```
runmqclsr -t tcp -m QM2
```

Pro odchozí připojení musíte kanál spustit jedním z následujících tří způsobů:

1. Použijte příkaz `MQSC START CHANNEL` a uveďte název kanálu, aby se kanál spustil jako proces nebo podproces, v závislosti na parametru `MCATYPE`. (Jsou-li kanály spouštěny jako podprocesy, jsou podprocesy iniciátoru kanálu.)

```
START CHANNEL(QM1.TO.QM2)
```

2. Pomocí příkazu `runmqchl` příkazu spusťte kanál jako proces.

```
runmqchl -c QM1.TO.QM2 -m QM1
```

3. Použijte inicializátor kanálu ke spuštění kanálu.

Zastavení kanálu

Použijte příkaz MQSC STOP CHANNEL, chcete-li požádat kanál o zastavení aktivity. Kanál nespustí novou dávku zpráv až do okamžiku, kdy operátor znovu spustí kanál.

Informace o restartování zastavených kanálů viz [“Restartování zastavených kanálů”](#) na stránce 162.

Tento příkaz lze zadat na kanál libovolného typu s výjimkou MQCHT_CLNTCONN.

Můžete vybrat typ zastavení, který vyžadujete:

Příklad příkazu pro zastavení

```
STOP CHANNEL(QM1.TO.QM2) MODE(QUIESCE)
```

Tento příkaz požaduje, aby se kanál zavřel spořádaným způsobem. Aktuální dávka zpráv je dokončena a procedura synchronizace se provádí s druhým koncem kanálu. Je-li kanál nečinný, tento příkaz neukončí přijímací kanál.

Příklad příkazu Stop force

```
STOP CHANNEL(QM1.TO.QM2) MODE(FORCE)
```

Tato volba ihned zastaví kanál, ale nezastavuje podproces nebo proces kanálu. Kanál nedokončí zpracování aktuální dávky zpráv, a proto může kanál v nejistém stavu opustit kanál. Obecně lze uvažovat o použití volby zastavení uvedení do klidového stavu.

Zastavit příklad ukončení

```
STOP CHANNEL(QM1.TO.QM2) MODE(TERMINATE)
```

Tato volba ihned zastaví kanál a ukončí vlákno nebo proces kanálu.

Zastavit (uvést do klidového stavu) příklad zastavení

```
STOP CHANNEL(QM1.TO.QM2) STATUS(STOPPED)
```

Tento příkaz neuvádí režim MODE, takže je výchozí nastavení MODE (QUIESCE). Požaduje, aby byl kanál zastaven, aby jej nebylo možné automaticky restartovat, ale musí být spuštěn ručně.

Příklad zastavení (uvedení do klidového stavu)

```
STOP CHANNEL(QM1.TO.QM2) STATUS(INACTIVE)
```

Tento příkaz neuvádí režim MODE, takže je výchozí nastavení MODE (QUIESCE). Požaduje, aby byl kanál deaktivován, aby se automaticky restartoval, je-li to nutné.

Přejmenování kanálu

K přejmenování kanálu zpráv použijte MQSC.

Použijte MQSC pro provedení následujících kroků:

1. Použijte příkaz STOP CHANNEL k zastavení kanálu.
2. Použijte příkaz DEFINE CHANNEL k vytvoření duplicitní definice kanálu s novým názvem.
3. Použijte příkaz DISPLAY CHANNEL, chcete-li zkontrolovat, zda byla vytvořena správně.

4. Použijte příkaz DELETE CHANNEL k odstranění původní definice kanálu.

Rozhodnete-li se přejmenovat kanál zpráv, nezapomeňte, že kanál má **dvě** definice kanálu, jeden na každém konci. Ujistěte se, že jste přejmenovali kanál na obou koncích současně.

Resetování kanálu

Chcete-li změnit pořadové číslo zprávy, použijte příkaz MQSC RESET CHANNEL.

Příkaz RESET CHANNEL je k dispozici pro všechny kanály zpráv, ale nikoli pro kanály MQI (připojení klienta nebo připojení k serveru). První zpráva začíná novou posloupností při příštím spuštění kanálu.

Je-li příkaz zadán na odesílacím nebo serverovém kanálu, informuje druhou stranu o změně kanálu po restartování kanálu.

Související pojmy

[“Začínáme s objekty” na stránce 176](#)

Kanály musí být definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál. Tento oddíl ukazuje, jak.

[“Řídící funkce kanálu” na stránce 152](#)

Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

[“Konfigurace distribuovaných front” na stránce 124](#)

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ, včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související informace

[Resetovat kanál](#)

Vyřešení nejistých zpráv na kanálu

Použijte příkaz MQSC RESOLVE CHANNEL, jsou-li zprávy zadrženy nejistou odesilatelem nebo serverem. Například, protože jeden konec odkazu byl ukončen a není zde žádná vyhlídka na obnovení.

Příkaz RESOLVE CHANNEL přijímá jeden ze dvou parametrů: BACKOUT nebo COMMIT. Funkce Backout obnovuje zprávy do přenosové fronty, zatímco operace Commit je vyřazuje.

Program kanálu se nepokusí o vytvoření relace s partnerem. Místo toho určí identifikátor logické jednotky práce (LUWID), který reprezentuje neověřené zprávy. Podle požadavku se pak vydává buď:

- BACKOUT pro obnovení zpráv do přenosové fronty; nebo
- COMMIT pro odstranění zpráv z přenosové fronty.

Aby bylo řešení úspěšné, postupujte takto:

- Kanál musí být neaktivní
- Kanál musí mít pochybnosti.
- Typ kanálu musí být odesílatel, server nebo odesílatel klastru.
- Definice lokálního kanálu musí existovat
- Lokální správce front musí být spuštěn.

Související pojmy

[“Začínáme s objekty” na stránce 176](#)

Kanály musí být definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál. Tento oddíl ukazuje, jak.

[“Řídící funkce kanálu” na stránce 152](#)

Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

[“Konfigurace distribuovaných front” na stránce 124](#)

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ, včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související informace

[Vyřešit kanál](#)

Nastavení komunikace pro Windows

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby to uspělo, je nezbytné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak to provést pomocí jedné ze čtyř forem komunikace pro systémy IBM MQ for Windows .

Může se stát, že vám pomůže se podívat na [Příklad konfigurace- IBM MQ for Windows](#) .

Pro systémy SYSTÉM UNIX a Linux viz [“Nastavení komunikace v systémech SYSTÉM UNIX a Linux” na stránce 190.](#)

Rozhodování o připojení

Vyberte si z následujících čtyř forem komunikace pro systémy IBM MQ for Windows :

- [“Definování připojení TCP na systému Windows” na stránce 183](#)
- [“Definování připojení LU 6.2 na systému Windows” na stránce 185](#)
- [“Definování připojení NetBIOS v systému Windows” na stránce 187](#)

Každá definice kanálu musí určovat pouze jeden protokol jako atribut Přenosový protokol (Typ transportu). Jeden nebo více protokolů může správce front použít.

Pro klienty IBM MQ může být užitečné mít alternativní kanály používající různé přenosové protokoly. Další informace o klientech IBM MQ naleznete v tématu [Přehled klientů](#).

Související pojmy

[“Konfigurace distribuovaných front” na stránce 124](#)

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

[“Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux” na stránce 173](#)

Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, aplikací IBM MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro synchronizační informace.

[“Konfigurace připojení mezi serverem a klientem” na stránce 14](#)

Chcete-li nakonfigurovat komunikační propojení mezi IBM MQ MQI clients a servery, rozhodněte se v komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

Definování připojení TCP na systému Windows

Definujte připojení TCP nakonfigurováním kanálu na odesílajícím konci, abyste určili adresu cíle, a spuštěním programu modulu listener na přijímajícím konci.

Odesílání: Konec

Do pole Název připojení v definici kanálu zadejte název hostitele nebo adresu TCP cílového počítače.

Port, který se má připojit, je výchozí hodnota 1414. Číslo portu 1414 je přiřazeno oprávnění Internet Assigned Numbers Authority k IBM MQ.

Chcete-li použít jiné číslo portu než výchozí, zadejte jej do pole názvu připojení v definici objektu kanálu takto:

```
DEFINE CHANNEL('channel name') CHLTYPE(SDR) +
    TRPTYPE(TCP) +
    CONNNAME('OS2R0G3(1822)') +
    XMITQ('XMitQ name') +
    REPLACE
```

kde OS2R0G3 je název DNS vzdáleného správce front a 1822 je požadovaný port. (Musí se jednat o port, na kterém naslouchá modul listener na přijímajícím konci.)

Spuštěný kanál musí být zastaven a restartován, aby se mohla změnit definice objektu kanálu. Výchozí číslo portu můžete změnit tak, že jej zadáte v souboru `.ini` pro produkt IBM MQ for Windows:

```
TCP:
Port=1822
```

Poznámka: Chcete-li vybrat číslo portu TCP/IP, které se má použít, použijte produkt IBM MQ první číslo portu, které nalezne, v následujícím pořadí:

1. Číslo portu explicitně určené v definici kanálu nebo v příkazovém řádku. Toto číslo umožňuje potlačení výchozího čísla portu pro kanál.
2. Atribut `port` uvedený ve stanze TCP souboru `.ini`. Toto číslo umožňuje přepsání výchozího čísla portu pro správce front.
3. Výchozí hodnota 1414. Toto je číslo přiřazené IBM MQ úřadem Internet Assigned Numbers Authority pro příchozí i odchozí připojení.

Další informace o hodnotách, které jste nastavili pomocí souboru `qm.ini`, najdete v tématu [Stanzy konfiguračního souboru pro distribuované ukládání do fronty](#).

Příjem na TCP

Chcete-li spustit přijímací program kanálu, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Můžete použít modul listener produktu IBM MQ .

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu.

Chcete-li spustit přijímací program kanálu, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Můžete použít modul listener produktu IBM MQ .

Chcete-li spustit modul listener dodávaný s produktem IBM MQ, který spouští nové kanály jako podprocesy, použijte příkaz `runmqclsr` .

Základní příklad použití příkazu **`runmqclsr`** :

```
runmqclsr -t tcp [-m QMNAME] [-p 1822]
```

Hranaté závorky označují volitelné parametry; `QMNAME` není vyžadováno pro výchozího správce front a číslo portu se nepožaduje, pokud používáte výchozí hodnotu (1414). Číslo portu nesmí být vyšší než 65535.

Poznámka: Chcete-li vybrat číslo portu TCP/IP, které se má použít, použijte produkt IBM MQ první číslo portu, které nalezne, v následujícím pořadí:

1. Číslo portu explicitně určené v definici kanálu nebo v příkazovém řádku. Toto číslo umožňuje potlačení výchozího čísla portu pro kanál.
2. Atribut `port` uvedený ve stanze TCP souboru `.ini`. Toto číslo umožňuje přepsání výchozího čísla portu pro správce front.
3. Výchozí hodnota 1414. Toto je číslo přiřazené IBM MQ úřadem Internet Assigned Numbers Authority pro příchozí i odchozí připojení.

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu [“Spuštění kanálů a listenerů jako důvěryhodných aplikací”](#) na stránce [173](#). Informace o důvěryhodných aplikacích najdete v tématu [Omezení pro důvěryhodné aplikace](#) .

Použití volby TCP/IP SO_KEEPALIVE

Chcete-li použít volbu Windows SO_KEEPALIVE, musíte do svého registru přidat následující položku:

```
TCP:  
KeepAlive=yes
```

Další informace o volbě SO_KEEPALIVE viz [“Kontrola, zda je druhý konec kanálu stále k dispozici” na stránce 159.](#)

V systému Windows hodnota registru

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters pro volbu času Windows KeepAlive řídí interval, který uplyne, než se bude kontrolovat připojení. Výchozí hodnota je dvě hodiny.

Použití volby nevyřízených požadavků na modul listener TCP

V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

Viz [“Použití volby nevyřízených požadavků na modul listener TCP” na stránce 192](#), kde získáte další informace, a specifickou hodnotu pro Windows.

Definování připojení LU 6.2 na systému Windows

Musí být konfigurována služba SNA, aby bylo možné mezi těmito dvěma počítači vytvořit konverzaci LU 6.2.

Po konfiguraci architektury SNA pokračujte následujícím způsobem.

Informace naleznete v následující tabulce.

Vzdálená platforma	TPNAME	TPPATH.
z/OS nebo MVS/ESA bez CICS	Totéž jako v příslušných vedlejších informacích o vzdáleném správci front.	-
z/OS nebo MVS/ESA pomocí CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-
IBM i	Stejně jako porovnávací hodnota v záznamu směrování v systému IBM i.	-
Systémy SYSTÉM UNIX a Linux	Totéž jako v příslušných vedlejších informacích o vzdáleném správci front.	MQ_INSTALLATION_PATH/bin/amqcrs6a
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nezvolitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.	MQ_INSTALLATION_PATH\bin\amqcrs6a

MQ_INSTALLATION_PATH představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ.

Pokud máte na jednom počítači více než jednoho správce front, ujistěte se, že názvy TPnames v definicích kanálů jsou jedinečné.

For the latest information about configuring AnyNet SNA over TCP/IP, see the following online IBM documentation: [AnyNet SNA přes TCP/IP](#) and [Obsluha uzlu SNA](#).

Související pojmy

[“Odeslání konce LU 6.2” na stránce 186](#)

Vytvořte objekt strany CPI-C (symbolické místo určení) z administrativní aplikace produktu LU 6.2 , kterou používáte. Zadejte tento název do pole Název připojení v definici kanálu. Také vytvořte odkaz LU 6.2 na partnera.

[“Příjem na LU 6.2” na stránce 186](#)

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu.

Odeslání konce LU 6.2

Vytvořte objekt strany CPI-C (symbolické místo určení) z administrativní aplikace produktu LU 6.2 , kterou používáte. Zadejte tento název do pole Název připojení v definici kanálu. Také vytvořte odkaz LU 6.2 na partnera.

V objektu strany CPI-C zadejte název partnerské LU na přijímajícím počítači, název TP a název režimu. Příklad:

```
Partner LU Name      OS2R0G2
Partner TP Name     recv
Mode Name           #INTER
```

Příjem na LU 6.2

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu.

Chcete-li spustit přijímací program kanálu, musí být spuštěn program listener, který zjistí příchozí požadavky na síť a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu RUNMQLSR, zadáním příkazu TpName , na kterém bude naslouchat. Případně můžete pro produkt Windows použít TpStart pod serverem SNA Server.

Použití příkazu RUNMQLSR

Příklad příkazu pro spuštění modulu listener:

```
RUNMQLSR -t LU62 -n RECV [-m QMNAME]
```

kde RECV je TpName , který je zadán na druhém konci (odesílání) jako "TpName ke spuštění na vzdálené straně". Poslední část v hranatých závorkách je volitelná a není vyžadována pro výchozího správce front.

Je možné mít více než jednoho správce front spuštěného na jednom počítači. Každému správci front je třeba přiřadit různé položky TpName a poté pro každou z nich spustit program modulu listener. Příklad:

```
RUNMQLSR -t LU62 -m QM1 -n TpName1
RUNMQLSR -t LU62 -m QM2 -n TpName2
```

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu [Spouštění kanálů a listenerů jako důvěryhodné aplikace](#). Informace o důvěryhodných aplikacích najdete v tématu [Omezení pro důvěryhodné aplikace](#) .

Všechny moduly listener produktu IBM MQ spuštěné ve správci front, který je neaktivní, můžete zastavit pomocí následujícího příkazu:

```
ENDMQLSR [-m QMNAME]
```

Použití serveru Microsoft SNA na systému Windows

Program TpSetup (ze sady SDK serveru SNA) můžete použít k definování vyvolaného TP, který pak vyvolá příkaz amqcrs6a.exe, nebo můžete ručně nastavit různé hodnoty registru. Parametry, které by měly být předány do souboru amqcrs6a.exe jsou:

```
-m QM -n TpName
```

kde *QM* je název správce front a *TpName* je název TP. Další informace naleznete v příručce *Microsoft SNA Server APPC Programmers Guide* nebo v příručce *Microsoft SNA Server CPI-C Programmers Guide*.

Nezadáte-li název správce front, bude předpokládán výchozí správce front.

Definování připojení NetBIOS v systému Windows

Produkt IBM MQ používá tři typy prostředků NetBIOS při vytváření připojení NetBIOS k jinému produktu IBM MQ : relace, příkazy a názvy. Každý z těchto prostředků má limit, který je standardně nastaven buď standardně, nebo volbou během instalace NetBIOS.

Každý běžící kanál, bez ohledu na typ, používá jednu relaci NetBIOS a jeden příkaz NetBIOS . Implementace NetBIOS produktu IBM umožňuje více procesům používat stejný lokální název NetBIOS . Proto musí být k dispozici pouze jeden název NetBIOS pro použití produktem IBM MQ. Implementace jiných dodavatelů, například emulace NetBIOS společnosti Novell, vyžadují pro každý proces odlišný lokální název. Ověřte své požadavky z dokumentace k produktu NetBIOS , který používáte.

Ve všech případech se ujistěte, že jsou již k dispozici dostatečné prostředky pro každý typ, nebo zvýšte maximální hodnoty uvedené v konfiguraci. Jakékoli změny hodnot vyžadují restart systému.

Během spouštění systému zobrazuje ovladač zařízení NetBIOS počet relací, příkazů a názvů, které jsou k dispozici pro použití aplikacemi. Tyto prostředky jsou k dispozici pro každou aplikaci založenou na systému NetBIOS, která je spuštěna na stejném systému. Proto je možné, aby jiné aplikace spotřebovávají tyto prostředky dříve, než je produkt IBM MQ potřebuje získat. Administrátor sítě LAN by vám to měl být schopen objasnit.

Související pojmy

[“Definování lokálního názvu NetBIOS produktu IBM MQ” na stránce 187](#)

Lokální název NetBIOS používaný procesy kanálu produktu IBM MQ lze určit třemi způsoby.

[“Vytváření omezení relací, příkazů a názvů správce front NetBIOS” na stránce 188](#)

Omezení správce front pro relace NetBIOS , příkazy a názvy lze zadat dvěma způsoby.

[“Zavedení čísla adaptéru LAN” na stránce 188](#)

Aby kanály fungovaly úspěšně napříč protokolem NetBIOS, musí být podpora adaptéru na každém konci kompatibilní. Produkt IBM MQ umožňuje řídit výběr čísla adaptéru LAN (LANA) pomocí hodnoty AdapterNum v sekci NETBIOS vašeho souboru qm.ini a zadáním parametru -a v příkazu runmqslr.

[“Inicializace připojení NetBIOS” na stránce 189](#)

Definování kroků potřebných k zahájení připojení.

[“Cílový modul listener pro připojení NetBIOS” na stránce 189](#)

Definování kroků, které mají být provedeny na přijímajícím konci připojení NetBIOS .

Definování lokálního názvu NetBIOS produktu IBM MQ

Lokální název NetBIOS používaný procesy kanálu produktu IBM MQ lze určit třemi způsoby.

V pořadí priorit jsou tyto tři způsoby:

1. Hodnota zadaná v parametru -l příkazu RUNMQLSR, například:

```
RUNMQLSR -t NETBIOS -l my_station
```

2. Proměnná prostředí MQNAME s hodnotou, která je vytvořena příkazem:

```
SET MQNAME= my_station
```

Pro každý proces můžete nastavit hodnotu MQNAME. Případně je můžete nastavit na úrovni systému v registru Windows .

Používáte-li implementaci NetBIOS , která vyžaduje jedinečné názvy, musíte v každém okně, ve kterém je spuštěn proces IBM MQ , zadat příkaz SET MQNAME. Hodnota MQNAME je libovolná, ale musí být jedinečná pro každý proces.

3. Oddíl NETBIOS v konfiguračním souboru správce front qm.ini. Příklad:

```
NETBIOS:  
LocalName= my_station
```

Poznámka:

1. Vzhledem k rozdílům v implementaci podporovaných produktů NetBIOS se doporučuje, aby se každý název NetBIOS každý v síti jedinečný. Pokud tak neuvidíte, může dojít k nepředvídatelným výsledkům. Pokud máte problémy se zavedením kanálu NetBIOS a v chybovém protokolu správce front jsou uvedeny chybové zprávy ukazující návratový kód NetBIOS X'15 ', zkontrolujte, zda používáte názvy NetBIOS .
2. V systému Windows nelze použít název počítače jako název NetBIOS , protože jej produkt Windows již používá.
3. Inicializace kanálu odesílatele vyžaduje, aby byl zadán název NetBIOS buď pomocí proměnné prostředí MQNAME, nebo pomocí proměnné LocalName v souboru qm.ini .

Vytváření omezení relací, příkazů a názvů správce front NetBIOS

Omezení správce front pro relace NetBIOS , příkazy a názvy lze zadat dvěma způsoby.

V pořadí přednosti jsou tyto způsoby:

1. Hodnoty zadané v příkazu RUNMQLSR:

```
-s Sessions  
-e Names  
-o Commands
```

Pokud v příkazu není zadán operand -m, použijí se hodnoty pouze pro výchozího správce front.

2. Oddíl NETBIOS v konfiguračním souboru správce front qm.ini. Příklad:

```
NETBIOS:  
  
NumSess= Qmgr_max_sess  
NumCmds= Qmgr_max_cmds  
NumNames= Qmgr_max_names
```

Zavedení čísla adaptéru LAN

Aby kanály fungovaly úspěšně napříč protokolem NetBIOS, musí být podpora adaptéru na každém konci kompatibilní. Produkt IBM MQ umožňuje řídit výběr čísla adaptéru LAN (LANA) pomocí hodnoty AdapterNum v sekci NETBIOS vašeho souboru qm.ini a zadáním parametru -a v příkazu runmqlsr.

Výchozí číslo adaptéru LAN použité produktem IBM MQ pro připojení NetBIOS je 0. Ověřte, jaké číslo se používá ve vašem systému, a to následujícím způsobem:

V systému Windows není možné zadávat dotazy na číslo adaptéru LAN přímo prostřednictvím operačního systému. Místo toho použijte LANACFG.EXE obslužný program příkazového řádku, dostupný z produktu Microsoft. Výstup nástroje zobrazuje čísla virtuálních adaptéru LAN a jejich účinné vazby. Další informace o číslech adaptéru LAN najdete v článku 138037 znalostní báze produktu Microsoft *HOWTO: Použití čísel LANA v 32bitovém prostředí*.

Určete správnou hodnotu v sekci NETBIOS konfiguračního souboru správce front qm.ini:

```
NETBIOS:  
AdapterNum= n
```

kde n je správné číslo adaptéru LAN pro tento systém.

Inicializace připojení NetBIOS

Definování kroků potřebných k zahájení připojení.

Chcete-li iniciovat připojení, proveďte následující kroky na odesílajícím konci:

1. Definujte název stanice NetBIOS pomocí hodnoty MQNAME nebo LocalName .
2. Ověřte, že číslo adaptéru LAN v systému je používáno, a zadejte správný soubor pomocí AdapterNum.
3. Do pole ConnectionName v definici kanálu zadejte název NetBIOS používaný cílovým programem modulu listener. V systému Windowsse kanály NetBIOS **musí** spouštět jako podprocesy. To lze provést zadáním parametru MCATYPE (THREAD) v definici kanálu.

```
DEFINE CHANNEL (chname) CHLTYPE(SDR) +  
TRPTYPE(NETBIOS) +  
CONNNAME(your_station) +  
XMITQ(xmitq) +  
MCATYPE(THREAD) +  
REPLACE
```

Cílový modul listener pro připojení NetBIOS

Definování kroků, které mají být provedeny na přijímajícím konci připojení NetBIOS .

Na přijímajícím konci proveďte následující kroky:

1. Definujte název stanice NetBIOS pomocí hodnoty MQNAME nebo LocalName .
2. Ověřte, že číslo adaptéru LAN v systému je používáno, a zadejte správný soubor pomocí AdapterNum.
3. Definujte přijímací kanál:

```
DEFINE CHANNEL (chname) CHLTYPE(RCVR) +  
TRPTYPE(NETBIOS) +  
REPLACE
```

4. Spuštěním programu modulu listener produktu IBM MQ vytvořte stanici a zpřístupněte ji tak, aby se s ní spojili. Příklad:

```
RUNMQLSR -t NETBIOS -l your_station [-m qmgr]
```

Tento příkaz ustanoví `your_station` jako stanici NetBIOS čekající na kontaktování. Název stanice NetBIOS musí být jedinečný v rámci sítě NetBIOS .

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu [“Spuštění kanálů a listenerů jako důvěryhodných aplikací”](#) na stránce [173](#). Informace o důvěryhodných aplikacích najdete v tématu [Omezení pro důvěryhodné aplikace](#) .

Všechny moduly listener produktu IBM MQ spuštěné ve správci front, který je neaktivní, můžete zastavit pomocí následujícího příkazu:

```
ENDMQLSR [-m QMNAME]
```

Nezadáte-li název správce front, bude předpokládán výchozí správce front.

Nastavení komunikace v systémech SYSTÉM UNIX a Linux

DQM je prostředek vzdáleného řazení do fronty pro produkt IBM MQ. Poskytuje řídicí programy kanálu pro správce front, které tvoří rozhraní pro komunikační propojení, ovladatelné systémem operátorem. Definice kanálů v rámci správy distribuovaných front používají tato připojení.

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nutné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak to provést. Může se také stát, že bude užitečné se podívat na následující oddíly:

- [Příklad konfigurace- IBM MQ for AIX](#)
- [Příklad konfigurace- IBM MQ for HP-UX](#)
- [Příklad konfigurace- IBM MQ for Solaris](#)
- [Příklad konfigurace- IBM MQ pro Linux](#)

Pro Windowsviz [“Nastavení komunikace pro Windows”](#) na stránce 183.

Můžete si vybrat mezi dvěma způsoby komunikace pro produkt IBM MQ v systémech SYSTÉM UNIX a Linux :

- [“Definování připojení TCP na systému SYSTÉM UNIX a Linux”](#) na stránce 190
- [“Definování připojení LU 6.2 na systému SYSTÉM UNIX a Linux”](#) na stránce 194

Každá definice kanálu musí určovat jeden pouze jako atribut přenosového protokolu (Typ transportu). Jeden nebo více protokolů může správce front použít.

Pro IBM MQ MQI clientsmůže být užitečné mít alternativní kanály používající různé přenosové protokoly. Další informace o produktu IBM MQ MQI clientsnaleznete v tématu [Přehled produktu IBM MQ MQI clients](#).

Související pojmy

[“Konfigurace distribuovaných front”](#) na stránce 124

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

[“Monitorování a řízení kanálů na platformách Windows, SYSTÉM UNIX a Linux”](#) na stránce 173

Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, aplikací IBM MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro synchronizační informace.

[“Konfigurace připojení mezi serverem a klientem”](#) na stránce 14

Chcete-li nakonfigurovat komunikační propojení mezi IBM MQ MQI clients a servery, rozhodněte se v komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

Definování připojení TCP na systému SYSTÉM UNIX a Linux

Definice kanálu na odesílajícím konci uvádí adresu cíle. Modul listener nebo démon inet je konfigurován pro připojení na konci příjmu.

Odesílání: Konec

Do pole Název připojení v definici kanálu zadejte název hostitele nebo adresu TCP cílového počítače. Port, který se má připojit, je výchozí hodnota 1414. Číslo portu 1414 je přiřazeno oprávnění Internet Assigned Numbers Authority k IBM MQ.

Chcete-li použít jiné číslo portu než výchozí, změňte pole s názvem připojení takto:

```
Connection Name REMHOST(1822)
```

kde REMHOST je název uzlu vzdáleného počítače a 1822 je číslo portu, které se požaduje. (Musí se jednat o port, na kterém naslouchá modul listener na přijímajícím konci.)

Další možností je změnit číslo portu jeho určením v konfiguračním souboru správce front (qm.ini):

```
TCP:
Port=1822
```

Další informace o hodnotách, které jste nastavili pomocí souboru `qm.ini`, najdete v tématu [Stanzy konfiguračního souboru pro distribuované ukládání do fronty](#).

Příjem na TCP

Můžete použít buď modul listener protokolu TCP/IP, který je démon `inet` (`inetd`), nebo modul listener produktu IBM MQ .

Některé distribuce Linux nyní používají rozšířený démon `inet` (`xinetd`) místo démona `inet`. Další informace o tom, jak používat rozšířený démon `inet` na systému Linux , najdete v tématu [Ustanovení připojení TCP na systému Linux](#) .

Související pojmy

[“Použití modulu listener protokolu TCP/IP” na stránce 191](#)

Chcete-li spustit kanály v systému SYSTÉM UNIX a Linux, je třeba upravit soubor `/etc/services` a soubor `inetd.conf` .

[“Použití volby nevyřízených požadavků na modul listener TCP” na stránce 192](#)

V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

[“Použití modulu listener produktu IBM MQ” na stránce 193](#)

Chcete-li spustit modul listener dodávaný s produktem IBM MQ, který spouští nové kanály jako podprocesy, použijte příkaz `runmq1sr` .

[“Použití volby TCP/IP SO_KEEPALIVE” na stránce 194](#)

Na některých systémech SYSTÉM UNIX a Linux můžete definovat, jak dlouho TCP čeká před kontrolou, zda je připojení stále dostupné, a jak často se znovu pokusí o připojení, pokud selže první kontrola. Je to buď laditelný parametr jádra, nebo jej lze zadat na příkazovém řádku.

Použití modulu listener protokolu TCP/IP

Chcete-li spustit kanály v systému SYSTÉM UNIX a Linux, je třeba upravit soubor `/etc/services` a soubor `inetd.conf` .

Postupujte podle těchto pokynů:

1. Upravte soubor `/etc/services` :

Poznámka: Chcete-li upravit soubor `/etc/services` , musíte být přihlášení jako uživatel `root` nebo uživatel `root`. Můžete to změnit, ale musí se shodovat s číslem portu uvedeným na konci odesílání.

Přidejte do souboru následující parametr:

```
MQSeries 1414/tcp
```

kde 1414 je číslo portu požadované produktem IBM MQ. Číslo portu nesmí být vyšší než 65535.

2. Přidejte řádek do souboru `inetd.conf` pro volání programu `amqcrsta`, kde `MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ :

```
MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta
[-m Queue_Man_Name]
```

Aktualizace jsou aktivní poté, co démon `inetd` znovu četl konfigurační soubory. Chcete-li to provést, zadejte následující příkazy z ID uživatele `root`:

- zapAIX:

```
refresh -s inetd
```

- Na serveru HP-UX ID uživatele mqm:

```
inetd -c
```

- V systémech Solaris 10 nebo novějších:

```
inetconv
```

- Na jiných systémech SYSTÉM UNIX a Linux (včetně Solaris 9):

```
kill -1 < process number >
```

Když program listener spuštěný démonem inetd dědí národní prostředí z inetd, je možné, že prostředí MQMDE není dodrženo (sloučeno) a je umístěno do fronty jako data zprávy. Abyste se ujistili, že je prostředí MQMDE uznáno, musíte nastavit národní prostředí správně. Národní prostředí nastavené inetd se nemusí shodovat s národním prostředím vybraným pro jiná národní prostředí používaná procesy IBM MQ . Nastavení národního prostředí:

1. Vytvořte skript shellu, který nastaví proměnné prostředí proměnné prostředí LANG, LC_COLLATE, LC_CTYPE, LC_MONETARY, LC_NUMERIC, LC_TIME a LC_MESSAGES na národní prostředí použité pro další proces IBM MQ .
2. Ve stejném skriptu shellu zavolejte program modulu listener.
3. Upravte soubor inetd.conf tak, aby volal váš skript shellu místo programu modulu listener.

Na serveru je možné mít více než jednoho správce front. Do každého z těchto dvou souborů musíte přidat řádek pro každého správce front. Příklad:

```
MQSeries1 1414/tcp
MQSeries2 1822/tcp
```

```
MQSeries2 stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta -m QM2
```

Kde `MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

Tím se vyvarujete generování chybových zpráv, pokud dojde k omezení počtu nevyřízených požadavků na připojení zařazených do fronty na jednom portu TCP. Informace o počtu neprovedených požadavků na připojení najdete v tématu [“Použití volby nevyřízených požadavků na modul listener TCP”](#) na stránce 192.

Použití volby nevyřízených požadavků na modul listener TCP

V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

Výchozí hodnoty nevyřízených požadavků listeneru jsou zobrazeny v [Tabulka 22](#) na stránce 192.

<i>Tabulka 22. Maximální počet nevyřízených požadavků na připojení zařazených do fronty na portu TCP/IP</i>	
Platforma serveru	Maximum požadavků na připojení
AIX	100
HP-UX	20

Tabulka 22. Maximální počet nevyřízených požadavků na připojení zařazených do fronty na portu TCP/IP (pokračování)

Platforma serveru	Maximum požadavků na připojení
Linux	100
IBM i	255
Solaris	100
Server Windows	100
Windows Pracovní stanice	100
z/OS	255

Pokud se nahromadění nevyřízených požadavků dosáhne hodnot zobrazených v [Tabulka 22 na stránce 192](#), připojení TCP/IP se odmítne a kanál se nebude moci spustit.

V případě kanálu MCA se tyto výsledky ve kanálu přejdou do stavu ZOPAKOVAT a znovu se pokusí o připojení později.

Chcete-li se však této chybě vyhnout, můžete přidat položku do souboru qm.ini :

```
TCP:  
ListenerBacklog = n
```

Tento parametr přepíše výchozí maximální počet nevyřízených požadavků (viz [Tabulka 22 na stránce 192](#)), pro modul listener protokolu TCP/IP.

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí. V případě potřeby lze tuto hodnotu použít, abyste se vyhnuli dosažení limitu připojení.

Chcete-li spustit modul listener s volbou backlog, přepnete na:

- Použijte příkaz `runmqtsr -b` nebo
- Použijte příkaz MQSC **DEFINE LISTENER** s atributem BACKLOG nastaveným na požadovanou hodnotu.

Informace o příkazu `runmqtsr` naleznete v části [runmqtsr](#). Další informace o příkazu DEFINE LISTENER naleznete v tématu [DEFINE LISTENER](#).

Použití modulu listener produktu IBM MQ

Chcete-li spustit modul listener dodávaný s produktem IBM MQ, který spouští nové kanály jako podprocesy, použijte příkaz `runmqtsr`.

Příklad:

```
runmqtsr -t tcp [-m QMNAME] [-p 1822]
```

Hranaté závorky označují volitelné parametry; QMNAME není vyžadováno pro výchozího správce front a číslo portu se nepožaduje, pokud používáte výchozí hodnotu (1414). Číslo portu nesmí být vyšší než 65535.

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu [“Spuštění kanálů a listenerů jako důvěryhodných aplikací”](#) na stránce [173](#). Informace o důvěryhodných aplikacích najdete v tématu [Omezení pro důvěryhodné aplikace](#).

Všechny moduly listener produktu IBM MQ spuštěné ve správci front, který je neaktivní, můžete zastavit pomocí následujícího příkazu:

```
endmqtsr [-m QMNAME]
```

Nezadáte-li název správce front, bude předpokládán výchozí správce front.

Použití volby TCP/IP SO_KEEPALIVE

Na některých systémech SYSTÉM UNIX a Linux můžete definovat, jak dlouho TCP čeká před kontrolou, zda je připojení stále dostupné, a jak často se znovu pokusí o připojení, pokud selže první kontrola. Je to buď laditelný parametr jádra, nebo jej lze zadat na příkazovém řádku.

Chcete-li použít volbu SO_KEEPALIVE (další informace viz [“Kontrola, zda je druhý konec kanálu stále k dispozici”](#) na stránce 159) Do konfiguračního souboru správce front (qm.ini) je třeba přidat následující položku:

```
TCP:
KeepAlive=yes
```

Další informace naleznete v dokumentaci k systému SYSTÉM UNIX a Linux .

Definování připojení LU 6.2 na systému SYSTÉM UNIX a Linux

Musí být konfigurována služba SNA, aby bylo možné mezi těmito dvěma počítači vytvořit konverzaci LU 6.2 .

Nejnovější informace o konfiguraci SNA přes TCP/IP najdete v následující online dokumentaci IBM : [Communications Server](#).

Musí být konfigurována služba SNA, aby bylo možné navázat konverzaci s LU 6.2 mezi dvěma systémy.

Informace naleznete v příručce *Multiplatform APPC Configuration Guide* a v následující tabulce.

Vzdálená platforma	TPNAME	TPPATH.
z/OS bez CICS	Stejně jako odpovídající TPName v informacích o připojení vzdáleného správce front.	-
z/OS použití CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-
IBM i	Stejně jako porovnávací hodnota v záznamu směrování v systému IBM i .	-
Systémy SYSTÉM UNIX a Linux	Stejně jako odpovídající TPName v informacích o připojení vzdáleného správce front.	<i>MQ_INSTALLATION_PATH/bin/amqcrs6a</i>
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nezvolnitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.	<i>MQ_INSTALLATION_PATH\bin\amqcrs6a</i>

MQ_INSTALLATION_PATH představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

Pokud máte na jednom počítači více než jednoho správce front, ujistěte se, že názvy TPnames v definicích kanálů jsou jedinečné.

Související pojmy

[“Odesílání: Konec”](#) na stránce 195

V systému SYSTÉM UNIX a Linux vytvořte objekt strany CPI-C (symbolické místo určení) a do pole Název připojení v definici kanálu zadejte tento název. Také vytvořte odkaz LU 6.2 na partnera.

[“Příjem na LU 6.2”](#) na stránce 195

Na systémech SYSTÉM UNIX a Linux vytvořte naslouchací přílohu na přijímajícím konci, profil logické připojení LU 6.2 a profil TPN.

Odesílání: Konec

V systému SYSTÉM UNIX a Linux vytvořte objekt strany CPI-C (symbolické místo určení) a do pole Název připojení v definici kanálu zadejte tento název. Také vytvořte odkaz LU 6.2 na partnera.

V bočním objektu CPI-C zadejte název partnerské LU na přijímajícím počítači, název transakčního programu a název režimu. Příklad:

```
Partner LU Name          REMHOST
Remote TP Name           recv
Service Transaction Program no
Mode Name                 #INTER
```

V systému HP-UX použijte proměnnou prostředí APPCLLU k pojmenování lokální LU, kterou by měl odesílatel používat. V systému Solaris nastavte proměnnou prostředí APPC_LOCAL_LU na název lokální LU.

SECURITY PROGRAM se používá, je-li podporován CPI-C, když se IBM MQ pokusí o zavedení relace SNA.

Příjem na LU 6.2

Na systémech SYSTÉM UNIX a Linux vytvořte naslouchací přílohu na přijímajícím konci, profil logické připojení LU 6.2 a profil TPN.

V profilu TPN zadejte úplnou cestu ke spustitelnému souboru a k názvu transakčního programu:

```
Full path to TPN executable  MQ_INSTALLATION_PATH/bin/amqcrs6a
Transaction Program name     recv
User ID                       0
```

`MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

V systémech, kde můžete nastavit ID uživatele, zadejte uživatele, který je členem skupiny mqm. V systémech AIX, Solaris a HP-UX nastavte proměnné prostředí APPCTPN (název transakce) a APPCLLU (název lokální LU) (můžete použít konfigurační panely pro vyvolaný transakční program).

Možná bude třeba použít jiného správce front, než je výchozí správce front. Pokud ano, definujte příkazový soubor, který volá:

```
amqcrs6a -m Queue_Man_Name
```

a pak zavolejte do příkazového souboru.

Monitorování a řízení kanálů v systému IBM i

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

Následující seznam je stručným popisem komponent funkce řízení kanálů:

- Definice kanálů jsou drženy jako objekty správce front.
- Příkazy kanálu jsou podmnožinou sady příkazů IBM MQ for IBM i .
Použijte příkaz GO CMDMQM k zobrazení úplné sady příkazů IBM MQ for IBM i .
- Použijte panely definice kanálu nebo příkazy pro:
 - Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálu
 - Spuštění a zastavení kanálů, testování spojení, resetování pořadových čísel kanálů a řešení sporných zpráv, pokud nelze znovu zavést propojení
 - Zobrazení informací o stavu kanálů

- Kanály lze také spravovat pomocí prostředí MQSC.
- Kanály lze také spravovat pomocí Průzkumníka IBM MQ
- Pořadová čísla a identifikátory *logické pracovní jednotky (LUW)* jsou uloženy v souboru synchronizace a používají se pro účely synchronizace kanálů.

Příkazy a panely můžete použít k definování kanálů zpráv a přidružených objektů a monitorování a řízení kanálů zpráv. Pomocí klávesy F4=Prompt můžete uvést odpovídajícího správce front. Pokud nepoužijete výzvu k zadání, předpokládá se výchozí správce front. S klávesou F4=Prompt se zobrazí další panel, na kterém můžete zadat příslušný název správce front a někdy i další data.

Objekty, které potřebujete definovat s panely, jsou:

- Přenosové fronty
- Definice vzdálených front
- Definice aliasů správce front
- Definice aliasů fronty odpovědí
- Odpovědi na lokální fronty
- Definice kanálů zpráv

Další informace o konceptech, které se podílejí na používání těchto objektů, najdete v tématu [“Konfigurace distribuovaných front”](#) na stránce 124.

Kanály musí být zcela definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál.

Kromě toho musí být pro každý kanál definován a dostupný konkrétní komunikační spoj, aby bylo možné kanál spustit. Popis toho, jak jsou definovány propojení LU 6.2 a TCP/IP, najdete v konkrétní komunikační příručce pro vaši instalaci.

Další informace o vytváření a práci s objekty naleznete v následujících tématech:

- [“Vytvoření objektů”](#) na stránce 196
- [“Vytvoření kanálu”](#) na stránce 197
- [“Spuštění kanálu”](#) na stránce 199
- [“Výběr kanálu”](#) na stránce 199
- [“Procházení kanálu”](#) na stránce 200
- [“Přejmenování kanálu”](#) na stránce 202
- [“Práce se stavem kanálu”](#) na stránce 202
- [“Práce s možností práce s kanálem”](#) na stránce 203

Související pojmy

[“Nastavení komunikace pro IBM MQ for IBM i”](#) na stránce 209

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby mohla být úspěšná, je nezbytné, aby připojení bylo definováno a dostupné.

[“Konfigurace připojení mezi serverem a klientem”](#) na stránce 14

Chcete-li nakonfigurovat komunikační propojení mezi IBM MQ MQI clients a servery, rozhodněte se v komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

Související informace

[Příklad konfigurace- IBM MQ for IBM i](#)

[Příklad plánování kanálů zpráv pro produkt IBM MQ for IBM i](#)

[Příkazy CL produktu IBM MQ for IBM i](#)

IBM i Vytvoření objektů

K vytvoření fronty a objektů aliasů můžete použít příkaz CRTMQMQ.

Můžete vytvořit frontu a objekty aliasu, jako jsou přenosové fronty, definice vzdálených front, definice alias správce front, definice aliasů fronty odpovědí a odpovědi na lokální fronty.

Seznam výchozích objektů najdete v tématu [Systémové a výchozí objekty systému IBM MQ for IBM i](#).

Vytvoření kanálu

Kanál můžete vytvořit z panelu Vytvořit kanál nebo pomocí příkazu CRTMQMCHL na příkazovém řádku.

Chcete-li vytvořit kanál:

1. Použijte F6 z panelu Práce s kanály MQM (WRKMQMCHL).

Případně použijte příkaz CRTMQMCHL z příkazového řádku.

Ať tak či onak, zobrazí se panel Vytvoření kanálu. Typ:

- Název kanálu v poskytnutém poli
- Typ kanálu pro tento konec odkazu

2. Stiskněte klávesu Enter.

Poznámka: Všechny kanály ve vaší síti musíte pojmenovat jedinečným způsobem. Jak je zobrazeno v [Síťový diagram zobrazující všechny kanály](#), včetně názvů zdrojového a cílového správce front v názvu kanálu je dobrý způsob, jak to provést.

Vaše položky se validují a chyby jsou nahlášeny okamžitě. Opravte všechny chyby a pokračujte.

Pro typ kanálu, který jste vybrali, se zobrazí příslušný panel nastavení kanálu. Vyplňte pole spolu s informacemi, které jste shromáždili dříve. Stisknutím klávesy Enter vytvoříte kanál.

Poskytujeme vám pomoc při rozhodování o obsahu různých polí v popisech panelů definice kanálu na panelech nápovědy a v části [Atributy kanálu](#).

```
Create MQM Channel (CRTMQMCHL)
Type choices, press Enter.

Channel name . . . . . > CHANNAME_____
Channel type . . . . . > *SDR__    *RCVR, *SDR, *SVR, *RQSTR...
Message Queue Manager name      *DFT_____

-----
Replace . . . . . *NO    *NO, *YES
Transport type . . . . . *TCP____ *LU62, *TCP, *SYSDFTCHL
Text 'description' . . . . . > 'Example Channel Definition'_____

-----
Connection name . . . . . *SYSDFTCHL_____
-----
-----
-----
-----
-----
-----
-----
-----
-----
-----
More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

Obrázek 25. Vytvořit kanál (1)

Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

```
Transmission queue . . . . . 'TRANSMISSION_QUEUE_NAME' _____
-----
Message channel agent . . . . . *NONE_____ Name, *SYSDFTCHL, *NONE
Library . . . . . _____ Name
Message channel agent user ID . *SYSDFTCHL__ Character value...
Coded Character Set Identifier *SYSDFTCHL__ 0-9999, *SYSDFTCHL
Batch size . . . . . 50_____ 1-9999, *SYSDFTCHL
Disconnect interval . . . . . 6000_____ 1-999999, *SYSDFTCHL
Short retry interval . . . . . 60_____ 0-999999999, *SYSDFTCHL
Short retry count . . . . . 10_____ 0-999999999, *SYSDFTCHL
Long retry interval . . . . . 1200_____ 0-999999999, *SYSDFTCHL
Long retry count . . . . . 999999999__ 0-999999999, *SYSDFTCHL
Security exit . . . . . *NONE_____ Name, *SYSDFTCHL, *NONE
Library . . . . . _____ Name
Security exit user data . . . . *SYSDFTCHL_____
-----
More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

Obrázek 26. Vytvořit kanál (2)

Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

```
Send exit . . . . . *NONE_____ Name, *SYSDFTCHL, *NONE
Library . . . . . _____ Name
+ for more values _____
Send exit user data . . . . . _____
+ for more values _____
Receive exit . . . . . *NONE_____ Name, *SYSDFTCHL, *NONE
Library . . . . . _____ Name
+ for more values _____
-----
Receive exit user data . . . . . _____
+ for more values _____
Message exit . . . . . *NONE_____ Name, *SYSDFTCHL, *NONE
Library . . . . . _____ Name
+ for more values _____
-----
More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

Obrázek 27. Vytvořit kanál (3)

Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

```
Message exit user data . . . . . -----
+ for more values -----
Convert message . . . . . *SYSDFTCHL_ *YES, *NO, *SYSDFTCHL
Sequence number wrap . . . . . 99999999__ 100-99999999, *SYSDFTCHL
Maximum message length . . . . . 4194304____ 0-4194304, *SYSDFTCHL
Heartbeat interval . . . . . 300_____ 0-99999999, *SYSDFTCHL
Non Persistent Message Speed . . *FAST_____ *FAST, *NORMAL, *SYSDFTCHL
Password . . . . . *SYSDFTCHL_ Character value, *BLANK...
Task User Profile . . . . . *SYSDFTCHL_ Character value, *BLANK...
Transaction Program Name . . . . *SYSDFTCHL
```

Bottom

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

Obrázek 28. Vytvořit kanál (4)

Spuštění kanálu

Kanál můžete spustit z panelu Práce s kanály nebo pomocí příkazu STRMQMCHL na příkazovém řádku.

Listenery jsou platné pouze pro TCP. Pro moduly listener SNA musíte nakonfigurovat komunikační subsystém.

Aby aplikace mohly vyměňovat zprávy, musíte spustit program listener pro příchozí připojení za použití příkazu STRMQMLSR.

V případě odchozích připojení je třeba kanál spustit jedním z následujících způsobů:

1. Použijte příkaz CL STRMQMCHL, který uvádí název kanálu, abyste spustili kanál jako proces nebo podproces, v závislosti na parametru MCATYPE. (Jsou-li kanály spouštěny jako podprocesy, jsou podprocesy iniciátoru kanálu.)

```
STRMQMCHL CHLNAME(QM1.TO.QM2) MQNAME(MYQMGR)
```

2. Použijte inicializátor kanálu ke spuštění kanálu. Inicializátor jednoho kanálu se spustí automaticky při spuštění správce front. Tento automatický start lze eliminovat změnou sekce chinit v souboru qm.ini pro daného správce front.
3. Použijte příkaz WRKMQMCHL pro zahájení práce s panelem Práce s kanály a vyberte volbu 14 pro spuštění kanálu.

Výběr kanálu

Kanál můžete vybrat na panelu Práce s kanály.

Chcete-li vybrat kanál, použijte příkaz WRKMQMCHL, abyste mohli začít na panelu Práce s kanály:

1. Přesuňte kurzor na pole voleb přidružené k požadovanému názvu kanálu.
2. Zadejte číslo volby.
3. Stisknutím klávesy Enter aktivujete svou volbu.

Vyberete-li více než jeden kanál, volby se aktivují v posloupnosti.

Work with MQM Channels

Queue Manager Name . . : CNX

Type options, press Enter.

2=Change 3=Copy 4=Delete 5=Display 8=Work with Status 13=Ping
14=Start 15=End 16=Reset 17=Resolve

Opt	Name	Type	Transport	Status
CHLNIC		*RCVR *TCP		INACTIVE
CORSAIR.TO.MUSTANG		*SDR	*LU62	INACTIVE
FV.CHANNEL.MC.DJE1		*RCVR	*TCP	INACTIVE
FV.CHANNEL.MC.DJE2		*SDR	*TCP	INACTIVE
FV.CHANNEL.MC.DJE3		*RQSTR	*TCP	INACTIVE
FV.CHANNEL.MC.DJE4		*SVR	*TCP	INACTIVE
FV.CHANNEL.PETER		*RCVR	*TCP	INACTIVE
FV.CHANNEL.PETER.LU		*RCVR	*LU62	INACTIVE
FV.CHANNEL.PETER.LU1		*RCVR	*LU62	INACTIVE

More...
Parameters or command
==>
F3=Exit F4=Prompt F5=Refresh F6=Create F9=Retrieve F12=Cancel
F21=Print

Obrázek 29. Práce s kanály

Procházení kanálu

Kanál můžete procházet z panelu Zobrazení kanálu nebo pomocí příkazu DSPMQMCHL na příkazovém řádku.

Chcete-li procházet nastavení kanálu, použijte příkaz WRKMQMCHL a začněte na panelu Zobrazení kanálu:

1. Zadejte volbu 5 (Zobrazení) proti požadovanému názvu kanálu.
2. Stisknutím klávesy Enter aktivujete svou volbu.

Vyberete-li více než jeden kanál, budou uvedeny v posloupnosti.

Případně můžete použít příkaz DSPMQMCHL z příkazového řádku.

Výsledkem je zobrazení příslušného panelu Zobrazení kanálu s podrobnostmi o aktuálních nastaveních pro kanál. Pole jsou popsána v části [Atributy kanálu](#).


```

Display MQM Channel

Channel name . . . . . : ST.JST.2T01
Queue Manager Name . . . . . : QMREL
Channel type . . . . . : *SDR
Transport type . . . . . : *TCP
Text 'description' . . . . . : John's sender to WINSDOA1

Connection name . . . . . : MUSTANG

Transmission queue . . . . . : WINSDOA1

Message channel agent . . . . . :
Library . . . . . :
Message channel agent user ID : *NONE
Batch interval . . . . . : 0
Batch size . . . . . : 50
Disconnect interval . . . . . : 6000

F3=Exit F12=Cancel F21=Print

```

Obrázek 30. Zobrazit kanál TCP/IP (1)

```

Display MQM Channel

Short retry interval . . . . . : 60
Short retry count . . . . . : 10
Long retry interval . . . . . : 6000
Long retry count . . . . . : 10
Security exit . . . . . :
Library . . . . . :
Security exit user data . . . . . :
Send exit . . . . . :
Library . . . . . :
Send exit user data . . . . . :
Receive exit . . . . . :
Library . . . . . :
Receive exit user data . . . . . :
Message exit . . . . . :
Library . . . . . :
Message exit user data . . . . . :
More...

F3=Exit F12=Cancel F21=Print

```

Obrázek 31. Zobrazit kanál TCP/IP (2)

```
Display MQM Channel
Sequence number wrap . . . . . : 999999999
Maximum message length . . . . : 10000
Convert message . . . . . : *NO
Heartbeat interval . . . . . : 300
Nonpersistent message speed . . *FAST
```

Bottom

F3=Exit F12=Cancel F21=Print

Obrázek 32. Zobrazit kanál TCP/IP (3)

Přejmenování kanálu

Kanál můžete přejmenovat z panelu Práce s kanály.

Chcete-li přejmenovat kanál zpráv, začněte na panelu Práce s kanály:

1. Ukončete kanál.
2. Použijte volbu 3 (Kopírování) pro vytvoření duplikátu s novým názvem.
3. Použijte volbu 5 (Zobrazení), abyste zkontrolovali, že byla vytvořena správně.
4. Použijte volbu 4 (Delete) k odstranění původního kanálu.

Pokud se rozhodnete přejmenovat kanál zpráv, ujistěte se, že oba konce kanálu jsou přejmenovány ve stejnou dobu.

Práce se stavem kanálu

S stavem kanálu můžete pracovat na panelu Práce se stavem kanálu.

Použijte příkaz WRKMQMCHST k zobrazení první sady panelů, které zobrazují stav vašich kanálů. Panely stavu v posloupnosti můžete zobrazit, když vyberete volbu Změnit zobrazení (F11).

Případně, výběrem volby 8 (Práce se stavem) z panelu Práce s kanály MQM se také zobrazí první stavový panel.

MQSeries Work with Channel Status

Type options, press Enter.

5=Display 13=Ping 14=Start 15=End 16=Reset 17=Resolve

Opt Name	Connection	Indoubt	Last Seq
CARTS_CORSAIR_CHAN	GBIBMIYA.WINSDOA1	NO	1
CHLNIC	9.20.2.213	NO	3
FV.CHANNEL.PETER2	9.20.2.213	NO	6225
JST.1.2	9.20.2.201	NO	28
MP_MUST_TO_CORS	9.20.2.213	NO	100
MUSTANG.TO.CORSAIR	GBIBMIYA.WINSDOA1	NO	10
MP_CORS_TO_MUST	9.20.2.213	NO	101
JST.2.3	9.5.7.126	NO	32
PF_WINSDOA1_LU62	GBIBMIYA.IYA80020	NO	54
PF_WINSDOA1_LU62	GBIBMIYA.WINSDOA1	NO	500
ST.JCW.EXIT.2T01.CHL	9.20.2.213	NO	216

Bottom

Parameters or command

==>

F3=Exit F4=Prompt F5=Refresh F6=Create F9=Retrieve F11=Change view

F12=Cancel F21=Print

Obrázek 33. První ze sady stavových panelů kanálu

Volby, které jsou k dispozici na panelu Práce se stavem kanálu, jsou:

Volba nabídky	Popis
5=Display	Zobrazí nastavení kanálu.
13=Ping	Inicializuje akci Ping, kde je to vhodné.
14=Start	Spustí kanál.
15=End	Zastaví kanál.
16=Reset	Vynuluje pořadové číslo kanálu.
17=Resolve	Řeší situaci v nejistém stavu, ručně.

Práce s možnostmi práce s kanálem

Panel Práce s kanály je dosažen příkazem WRKMQMCHL a umožňuje vám monitorovat stav všech vypsanych kanálů a vydávat příkazy proti vybraným kanálům.

Volby, které jsou k dispozici na panelu Práce s kanály, jsou:

Volba nabídky	Popis
<u>"2=Change" na stránce 204</u>	Změní atributy kanálu.
<u>"3=Copy" na stránce 204</u>	Zkopíruje atributy kanálu do nového kanálu.
<u>"4=Delete" na stránce 204</u>	Odstraní kanál.
<u>"5=Display" na stránce 204</u>	Zobrazí aktuální nastavení pro kanál.
<u>"6=Create" na stránce 204</u>	Zobrazí panel Vytvořit kanál
<u>"8=Work se stavem" na stránce 205</u>	Zobrazí stavové panely kanálu.

Volba nabídky	Popis
<u>“13=Ping” na stránce 206</u>	Spustí poskytovanou službu PING tak, aby otestuje spojení se sousedním systémem pomocí výměny pevné datové zprávy se vzdáleným koncem.
<u>“14=Start” na stránce 206</u>	Spustí vybraný kanál nebo resetuje zablokovaný přijímací kanál.
<u>“15=End” na stránce 207</u>	Požaduje uzavření kanálu.
<u>“16=Reset” na stránce 208</u>	Požaduje, aby kanál resetoval pořadová čísla na tomto konci spojení. Čísla musí být stejná na obou koncích, aby se kanál mohl spustit.
<u>“17=Resolve” na stránce 208</u>	Požaduje, aby kanál interpretoval neověřené zprávy bez navázání spojení s druhým koncem.
<u>“18=Zobrazení oprávnění” na stránce 208</u>	Zobrazí oprávnění k objektu IBM MQ
<u>“19=Udělení oprávnění” na stránce 208</u>	Uděluje oprávnění k objektu IBM MQ
<u>“20=Odvolání oprávnění” na stránce 208</u>	Odvolá oprávnění k objektu IBM MQ
<u>“21=Zotavit objekt” na stránce 208</u>	Obnovený objekt IBM MQ
<u>“22=Záznam obrazu” na stránce 209</u>	Obraz objektu IBM MQ záznamů

2=Change

Chcete-li změnit existující definici kanálu, použijte volbu Změna.

Volba Změna, nebo příkaz CHGMQMCHL mění existující definici kanálu, kromě názvu kanálu. Přepište pole, která se mají změnit na panelu definice kanálu, a poté uložte aktualizovanou definici stisknutím klávesy Enter.

3=Copy

Použijte volbu Kopírovat ke kopírování existujícího kanálu.

Volba Kopírování používá příkaz CPYMQMCHL ke kopírování existujícího kanálu. Panel Kopírování vám umožňuje definovat nový název kanálu. Tyto znaky však musíte omezit na znaky, které jsou platné pro názvy objektů produktu IBM MQ for IBM i, viz *Správa systému IBM MQ for IBM i*.

Stisknutím klávesy Enter na panelu Kopírování zobrazíte podrobnosti o aktuálních nastaveních. Můžete změnit libovolné nové nastavení kanálu. Novou definici kanálu uložte stisknutím klávesy Enter.

4>Delete

Chcete-li odstranit vybraný kanál, použijte volbu Odstranit.

Zobrazí se panel pro potvrzení nebo zrušení vašeho požadavku.

5=Display

Pomocí volby Zobrazit můžete zobrazit aktuální definice pro kanál.

Tato volba zobrazí panel s poli zobrazenými aktuálními hodnotami parametrů a chráněný proti vstupu uživatele.

6=Create

Pomocí volby Create můžete zobrazit panel Vytvořit kanál.

Použijte volbu Create, nebo zadejte příkaz CRTMQMCHL z příkazového řádku, abyste získali panel Vytvořit kanál. K dispozici jsou příklady panelů Vytvořit kanál, které začínají v [Obrázek 25 na stránce 197](#).

Prostřednictvím tohoto panelu můžete vytvořit definici kanálu z obrazovky polí vyplněných výchozími hodnotami dodanými produktem IBM MQ for IBM i. Zadejte název kanálu, vyberte typ kanálu, který vytváříte, a metodu komunikace, která má být použita.

Stisknete-li Enter, zobrazí se panel. Zadejte informace do všech požadovaných polí na tomto panelu a zbývající panely a poté uložte definici stisknutím klávesy Enter.

Název kanálu musí být stejný na obou koncích kanálu a musí být jedinečný v rámci sítě. Musíte však omezit znaky použité na tyto znaky, které jsou platné pro názvy objektů produktu IBM MQ for IBM i.

Pro některá pole mají všechny panely výchozí hodnoty zadané v produktu IBM MQ for IBM i. Tyto hodnoty můžete upravit, nebo je můžete změnit, když vytváříte nebo kopírujete kanály. Chcete-li upravit hodnoty, podívejte se na *IBM MQ for IBM i System Administration*.

Můžete vytvořit vlastní sadu výchozích hodnot kanálu tak, že nastavíte fiktivní kanály s požadovanými výchozími hodnotami pro každý typ kanálu a zkopírujete je pokaždé, když chcete vytvořit nové definice kanálu.

Související informace

[Atributy kanálu](#)

8=Work se stavem

Chcete-li zobrazit podrobné informace o stavu kanálu, použijte volbu Práce se stavem.

Sloupec Stav informuje o tom, zda je kanál aktivní nebo neaktivní, a že je průběžně zobrazen na panelu Práce s kanály MQM. Použijte volbu 8 (Práce se stavem), abyste viděli více zobrazených informací o stavu. Alternativně lze tyto informace zobrazit z příkazového řádku pomocí příkazu WRKMQMCHST. Viz [“Práce se stavem kanálu” na stránce 202](#).

- Název kanálu
- Typ kanálu
- Stav kanálu
- Instance kanálu
- Vzdálený správce front
- Jméno přenosové fronty
- Název komunikačního připojení
- Stav nejistého stavu kanálu
- Poslední pořadové číslo
- Počet nejistých zpráv
- Pořadové číslo, které vyvolává pochybnosti
- Počet zpráv v přenosové frontě
- Identifikátor logické pracovní jednotky
- Identifikátor logické pracovní jednotky v nejistém stavu
- Dílčí stav kanálu
- Monitorování kanálů
- Kompresce záhlaví
- Kompresce zpráv
- Indikátor doby komprese
- Ukazatel míry komprese
- Indikátor doby přenosové fronty
- Indikátor doby sítě

- Indikátor času ukončení
- Indikátor velikosti dávky
- Aktuální sdílené konverzace
- Maximum sdílených konverzací

13=Ping

Použijte volbu PING k výměně pevné datové zprávy se vzdáleným koncem.

A successful IBM MQ Ping gives some confidence to the system supervisor that the channel is available and functioning.

Příkaz ping nezahrnuje použití přenosových front a cílových front. Používá definice kanálu, související komunikační linku a nastavení sítě.

Je k dispozici pouze pro kanály odesílatele a serveru. Odpovídající kanál se spustí na vzdálené straně odkazu a provede dohodnutí spouštěcího parametru. Chyby jsou oznámeny normálně.

Výsledek výměny zpráv se zobrazí na panelu PING pro vás a je vráceným textem zprávy spolu s časem odeslání zprávy a časem přijetí odpovědi.

Příkaz ping s LU 6.2

Je-li příkaz PING vyvolán v produktu IBM MQ for IBM i, spouští se s ID uživatele požadujícího funkci, zatímco normální způsob, jakým je spuštěn program kanálu, je určen pro ID uživatele QMQM, které má být převzato pro kanály kanálu. ID uživatele proudí do přijímající strany a musí být platné na přijímajícím konci konverzace LU 6.2 , která má být alokována.

14=Start

Chcete-li spustit kanál ručně, použijte volbu Spustit.

Volba Start je k dispozici pro kanály odesílatele, serveru a žadatele. Není nutné, aby byl kanál nastaven se spuštěním správce front.

Volba Start se také používá pro kanály příjemce, připojení k serveru, odesílatele klastru a příjemce klastru. Spuštění přijímacího kanálu, který je ve stavu STOPPED, znamená, že jej lze spustit ze vzdáleného kanálu.

Když je spuštěna, odesílající agent MCA přečte definiční soubor kanálu a otevře přenosovou frontu. Je vydána spouštěcí posloupnost kanálu, která vzdáleně spustí odpovídající MCA přijímače nebo kanálu serveru. Po spuštění budou procesy odesílatele a serveru čekat na zprávy přicházející do přenosové fronty a předávají je, jakmile dorazí.

Když používáte spouštěcí impuls, musíte spustit stále běžící spouštěcí proces, abyste monitorovali inicializační frontu. Příkaz STRMQMCHLI lze použít pro spuštění procesu.

Na vzdáleném konci kanálu může být přijímající proces spuštěn jako odezva na spuštění kanálu z odesílajícího konce. Tato metoda se liší pro LU 6.2 a TCP/IP připojené kanály:

- LU 6.2 připojených kanálů nevyžaduje žádnou explicitní akci na přijímajícím konci kanálu.
- Připojené kanály protokolu TCP vyžadují, aby byl proces modulu listener spuštěn nepřetržitě. Tento proces čeká na požadavky na spuštění kanálu od vzdáleného konce odkazu a spustí proces definovaný v definicích kanálu pro dané připojení.

Je-li vzdálený systém IBM i, můžete použít příkaz STRMQMLSR.

Použití volby Start vždy způsobí, že se kanál resynchronizuje, je-li to nutné.

Aby bylo možné začít úspěšně:

- Definice kanálů, lokální a vzdálené musí existovat. Pokud neexistuje vhodná definice kanálu pro přijímací kanál nebo kanál připojení serveru, vytvoří se automaticky, je-li kanál automaticky definován, automaticky. Viz [Channel auto-definition exit program](#).

- Přenosová fronta musí existovat, musí být povolena pro GET a nemají žádné jiné kanály používající ji.
- MCAs, místní a vzdálený, musí existovat.
- Komunikační spojení musí být dostupné.
- Správci front musí být spuštěni, lokálními a vzdálenými.
- Kanál zpráv musí být neaktivní.

Chcete-li přenášet zprávy, vzdálené fronty a definice vzdálených front musí existovat.

Zobrazí se panel potvrzující, že požadavek na spuštění kanálu byl přijat. Chcete-li potvrdit, že úvodní proces byl úspěšný, zkontrolujte systémový protokol nebo stiskněte klávesu F5 (obnovte obrazovku).

15=End

Aktivita kanálu slouží k zastavení aktivity kanálu.

Pomocí volby Ukončit lze požádat kanál o zastavení aktivity. Kanál neodešle žádné další zprávy.

Před stisknutím klávesy Enter vyberte volbu F4 a zvolte, zda se kanál stane ZASTAVENO nebo NEAKTIVNÍ, a zda má být kanál zastaven pomocí ŘADIČE nebo zastavení IMMEDIATE. Zastavený kanál musí být znovu spuštěn operátorem, aby se znovu aktivoval. Může být spuštěn neaktivní kanál.

Okamžité zastavení

Použijte okamžité zastavení k zastavení kanálu bez dokončení libovolné jednotky práce.

Tato volba ukončuje proces kanálu. Výsledkem je, že kanál nedokončí zpracování aktuální dávky zpráv, a proto nemůže kanál v nejistém stavu opustit kanál. Obecně platí, že je lepší, aby operátoři mohli používat volbu řízeného zastavení.



Zastavit řízené

Pomocí příkazu Stop lze zastavit kanál na konci aktuální jednotky práce.


Tato volba požaduje, aby kanál byl ukončen řádným způsobem; aktuální dávka zpráv je dokončena a procedura synchronizačního bodu se provádí s druhým koncem kanálu.


Restartování zastavených kanálů

Když kanál přejde do stavu ZASTAVENO, je třeba kanál restartovat ručně. Kanál můžete restartovat následujícími způsoby:

- Pomocí příkazu **START CHANNEL MQSC**.
- Pomocí příkazu **Start Channel PCF**.
- Pomocí produktu MQ Explorer.
-  V systému z/OS pomocí panelu Spustit kanál.
-  V systému IBM i pomocí příkazu **STRMQMCHL CL** nebo volby **ZAČÁTEK** na panelu WRKMQMCHL.

V případě odesílatelů nebo kanálů serveru, kdy kanál vstoupil do stavu STOPPED, byla přidružená přenosová fronta nastavena na GET (DISABLED) a spuštění bylo vypnuto. Když je přijat požadavek na spuštění, tyto atributy se resetují automaticky.

 Pokud se inicializátor kanálu zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu inicializátoru kanálu. Stav kanálu pro typ kanálu SVRCONN se však resetuje, pokud se zastaví inicializátor kanálu v době, kdy je kanál ve stavu ZASTAVENO.

 Pokud se správce front zastaví v případě, že se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu správce front. Počínaje verzí IBM MQ

Verze 8.0 se tato volba vztahuje také na kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

16=Reset

Chcete-li vynutit novou posloupnost zpráv, použijte volbu Reset.

Volba Reset změní pořadové číslo zprávy. Používejte jej opatrně a pouze poté, co jste použili volbu Vyřešit k vyřešení všech situací, které jsou v nejistém stavu. Tato volba je k dispozici pouze u odesílacího kanálu nebo kanálu serveru. První zpráva začíná novou posloupností při příštím spuštění kanálu.

17=Resolve

Použijte volbu Vyřešit, abyste vynutili lokální potvrzení nebo vrácení neověřených zpráv, které se nacházejí v přenosové frontě.

Použijte volbu Vyřešit, když zprávy jsou drženy v nejistém stavu odesilatelem nebo serverem, například protože jeden konec odkazu byl ukončen a není zde žádná vyhlídka na obnovení. Volba Vyřešit přijímá jeden ze dvou parametrů: BACKOUT nebo COMMIT. Funkce Backout obnovuje zprávy do přenosové fronty, zatímco operace Commit je vyřazuje.

Program kanálu se nepokusí o vytvoření relace s partnerem. Místo toho určí identifikátor logické jednotky práce (LUWID), který reprezentuje neověřené zprávy. Podle požadavku se pak vydává buď:

- BACKOUT pro obnovení zpráv do přenosové fronty; nebo
- COMMIT pro odstranění zpráv z přenosové fronty.

Aby bylo řešení úspěšné, postupujte takto:

- Kanál musí být neaktivní
- Kanál musí mít pochybnosti.
- Typ kanálu musí být odesílatel nebo server
- Definice kanálu, lokální, musí existovat
- Správce front musí být spuštěn, lokální

18=Zobrazení oprávnění

Volbu Zobrazení oprávnění použijte k zobrazení toho, jaké akce má uživatel oprávnění provádět na specifickém objektu IBM MQ .

Pro vybraný objekt a uživatele zobrazí příkaz DSPMQAUT oprávnění, která má uživatel k provádění akcí na objektu IBM MQ . Je-li uživatel členem více skupin, pak příkaz zobrazí kombinovanou autorizaci všech skupin k objektu.

19=Udělení oprávnění

Použijte volbu Udělit oprávnění, abyste udělili oprávnění provádět akce s objekty IBM MQ jinému uživateli nebo skupině uživatelů.

Příkaz GRMQMAUT je k dispozici pouze pro uživatele ve skupině QMQMADM. Uživatel v QMQMADM uděluje oprávnění jiným uživatelům provádět akce na objektech IBM MQ uvedených v příkazu buď identifikací uživatelů podle jména, nebo udělením oprávnění všem uživatelům v *PUBLIC.

20=Odvolání oprávnění

Oprávnění k odebrání oprávnění k provádění akcí na objektech od uživatelů lze odebrat pomocí oprávnění Odebrat oprávnění.

Příkaz RVKMQMAUT je k dispozici pouze pro uživatele ve skupině QMQMADM. Uživatel ve skupině QMQMADM odstraní oprávnění od jiných uživatelů k provádění akcí na objektech IBM MQ vyjmenovaných v příkazu buď identifikováním uživatelů podle jména, nebo zrušením oprávnění od všech uživatelů v *PUBLIC.

21=Zotavit objekt

Použijte Obnova objektu k obnově poškozených objektů z informací uložených v žurnálech IBM MQ .

Obnova objektu používá příkaz RCRMQMOBJ (Re-create MQ Object) k obnově všech objektů, které jsou v příkazu poškozeny. Pokud objekt není poškozen, neprovede se žádná akce na daném objektu.

22=Záznam obrazu

Použijte obraz záznamu ke snížení počtu žurnálových zásobníků požadovaných pro obnovu sady objektů a k minimalizaci doby obnovy.

Příkaz RCDMQMIMG má kontrolní bod pro všechny objekty, které jsou vybrány v příkazu. Synchronizuje aktuální hodnoty objektů v integrovaném systému souborů (IFS) s pozdějšími informacemi o objektech, jako jsou operace MQPUTs a MQGET zaznamenané v žurnálových zásobnících.

Když příkaz dokončí objekty v IFS, jsou aktuální a tyto žurnálové zásobníky již nemusí být přítomny, aby mohly být objekty napraveny. Všechny odpojené žurnálové zásobníky mohou být odpojeny (pokud není požadováno, aby mohly být přítomny pro obnovu jiných objektů).

Nastavení komunikace pro IBM MQ for IBM i

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby mohla být úspěšná, je nezbytné, aby připojení bylo definováno a dostupné.

DQM je prostředek vzdáleného řazení do fronty pro produkt IBM MQ for IBM i. Poskytuje řídicí programy kanálu pro správce front produktu IBM MQ for IBM i, které tvoří rozhraní pro komunikační spojení, které lze řídit operátorem systému.

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby mohla být úspěšná, je nezbytné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak zajistit, aby připojení bylo definováno a dostupné.

Před spuštěním kanálu musí být přenosová fronta definována způsobem popsaným v této části a musí být zahrnuta do definice kanálu zpráv.

Můžete si vybrat mezi následujícími dvěma způsoby komunikace mezi systémy IBM MQ for IBM i :

- [“Definování připojení TCP na systému IBM i” na stránce 210](#)

Pro protokol TCP lze použít adresu hostitele a tato připojení jsou nastavena tak, jak je popsáno v příručce *IBM i Communication Configuration Reference*.

V prostředí TCP je každá distribuovaná služba alokována jedinečnou adresou TCP, kterou mohou používat vzdálené počítače pro přístup ke službě. Adresa TCP se skládá z názvu hostitele/čísla a čísla portu. Všichni správci front používají takové číslo ke vzájemné komunikaci prostřednictvím protokolu TCP.

- [“Příjem na TCP” na stránce 210](#)

Tato forma komunikace vyžaduje definici logické jednotky IBM i SNA typu 6.2 (LU 6.2), která poskytuje fyzický spoj mezi systémem IBM i obsluhujícím lokálního správce front a systémem obsluhujícím vzdáleného správce front. Podrobnosti o konfiguraci komunikací v produktu IBM inajdete v příručce *IBM i Communication Configuration Reference*.

Kromě toho musí být v případě potřeby připravován spouštěcí mechanismus s definicí nezbytných procesů a front.

Související pojmy

[“Monitorování a řízení kanálů v systému IBM i” na stránce 195](#)

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

Související informace

[Příklad konfigurace- IBM MQ for IBM i](#)

[Příklad plánování kanálů zpráv pro produkt IBM MQ for IBM i](#)

[Interkomunikační úlohy v systému IBM i](#)

[Stav kanálů v systému IBM i](#)

Definování připojení TCP na systému IBM i

V rámci definice kanálu můžete definovat připojení TCP pomocí pole *Název připojení*.

Definice kanálu obsahuje pole *CONNECTION NAME*, které obsahuje buď síťovou adresu TCP cíle, nebo název hostitele (například ABCHOST). Síťová adresa TCP může být v tečkovém desítkovém tvaru IPv4 (například 127.0.0.1) nebo v hexadecimální formě IPv6 (například 2001:DB8:0:0:0:0:0). Pokud je *NÁZEV PŘIPOJENÍ* název hostitele nebo server názvů, tabulka hostitelů IBM i se používá k převedení názvu hostitele na adresu hostitele TCP.

Číslo portu je povinné pro úplnou adresu TCP; pokud toto číslo není dodáno, použije se výchozí číslo portu 1414. Na zahajovacím konci připojení (typy kanálů odesílatele, žadatele a serveru) je možné poskytnout volitelné číslo portu pro připojení, například:

```
Connection name 127.0.0.1 (1555)
```

V tomto případě se iniciující ukončení pokusí připojit k přijímajícímu programu na portu 1555.

Použití volby nevyřízených požadavků na modul listener TCP

V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

Viz [“Použití volby nevyřízených požadavků na modul listener TCP”](#) na stránce 192, kde získáte další informace, a specifickou hodnotu pro IBM i.

Související pojmy

[“Příjem na TCP”](#) na stránce 210

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu. Chcete-li odpovědět na požadavek na spuštění, je třeba spustit program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu STRMQMLSR.

Příjem na TCP

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu. Chcete-li odpovědět na požadavek na spuštění, je třeba spustit program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu STRMQMLSR.

Pro každého správce front můžete spustit více než jeden modul listener. Ve výchozím nastavení příkaz STRMQMLSR používá port 1414, ale tuto hodnotu můžete přepsat. Chcete-li přepsat výchozí nastavení, přidejte následující příkazy do souboru qm.ini vybraného správce front. V tomto příkladu je listener požadován pro použití portu 2500:

```
TCP:  
Port=2500
```

Soubor qm.ini se nachází v tomto adresáři IFS: */QIBM/UserData/mqm/qmgrs/ název správce front*.

Tato nová hodnota se načte pouze v případě, že je spuštěn modul listener TCP. Máte-li již spuštěný modul listener, nebude tento program tento program vidět. Chcete-li použít novou hodnotu, zastavte modul listener a znovu zadejte příkaz STRMQMLSR. Nyní, kdykoli použijete příkaz STRMQMLSR, je listener standardně nastaven na nový port.

Případně můžete zadat jiné číslo portu v příkazu STRMQMLSR. Příklad:

```
STRMQMLSR MQMNAME( queue manager name ) PORT(2500)
```

Tato změna způsobí, že modul listener bude standardně nastaven na nový port po dobu trvání úlohy modulu listener.

Použití volby TCP SO_KEEPALIVE

Chcete-li použít volbu SO_KEEPALIVE (další informace viz [“Kontrola, zda je druhý konec kanálu stále k dispozici”](#) na stránce 159) Do konfiguračního souboru správce front (qm.ini v adresáři IFS, /QIBM/UserData/mqm/qmgrs/ *název správce front*) je třeba přidat následující položku:

```
TCP:
KeepAlive=yes
```

Pak musíte zadat následující příkaz:

```
CFGTCP
```

Vyberte volbu 3 (Change TCP Attributes). Nyní můžete zadat časový interval v minutách. Můžete zadat hodnotu v rozsahu 1 až 40320 minut; výchozí hodnota je 120.

Použití volby nevyřízených požadavků na modul listener TCP

Při příjmu na protokolu TCP je nastaven maximální počet neprovedených požadavků na připojení. Toto číslo může být považováno za *nevyřízené požadavky* požadavků čekajících na port TCP pro modul listener, aby přijal požadavek.

Výchozí hodnota nahromadění modulu listener v systému IBM i je 255. Pokud velikost nevyřízených požadavků dosáhne této hodnoty, připojení TCP se odmítne a kanál nebude možné spustit.

V případě kanálu MCA se výsledkem tohoto výsledku v kanálu stane stav ZOPAKOVAT a později se znovu pokusí o připojení.

V případě připojení klienta obdrží klient kód příčiny MQRQ_Q_MGR_NOT_AVAILABLE z objektu MQCONN a později se může připojení pokusit o zopakování připojení.

Chcete-li se však této chybě vyhnout, můžete přidat položku do souboru qm.ini :

```
ListenerBacklog = n
```

Tento parametr přepíše výchozí maximální počet nevyřízených požadavků (255) pro modul listener TCP.

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí. V případě potřeby lze tuto hodnotu použít, abyste se vyhnuli dosažení limitu připojení.

Definování připojení LU 6.2 na systému IBM i

Definujte podrobnosti o komunikaci LU 6.2 pomocí názvu režimu, názvu TP a názvu připojení pro plně kvalifikované připojení LU 6.2 .

Iniciovaný konec odkazu musí mít definici směrovacího záznamu, aby doplňoval tento objekt CSI. Další informace o správě pracovních požadavků ze vzdálených logických jednotek LU 6.2 jsou k dispozici v příručce *IBM i Programming: Work Management Guide*.

Informace naleznete v příručce *Multiplatform APPC Configuration Guide* a v následující tabulce.

Vzdálená platforma	TPNAME
z/OS nebo MVS	Totéž jako v příslušných vedlejších informacích o vzdáleném správcí front.
IBM i	Stejně jako porovnávací hodnota v záznamu směrování v systému IBM i .
HP Integrity NonStop Server	Stejně jako název TPNAME uvedený v definici kanálu příjemce.

<i>Tabulka 24. Nastavení na lokálním systému IBM i pro vzdálenou platformu správce front (pokračování)</i>	
Vzdálená platforma	TPNAME
Systémy SYSTÉM UNIX a Linux	Invovatelný transakční program definovaný ve vzdálené konfiguraci LU 6.2 .
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nezvolitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.

Pokud máte ve stejném počítači více než jednoho správce front, ujistěte se, že názvy TPnames v definicích kanálů jsou jedinečné.

Související pojmy

“Zahájení ukončení (Odesílatel)” na stránce 212

Použijte příkaz CRTMQMCHL, abyste definovali kanál typu přenosu *LU62.

“Iniciování konce (přijímač)” na stránce 214

Použijte příkaz CRTMQMCHL, abyste definovali přijímací konec propojení kanálu zpráv s typem přenosu *LU62.

Zahájení ukončení (Odesílatel)

Použijte příkaz CRTMQMCHL, abyste definovali kanál typu přenosu *LU62.

Použití objektu CSI je volitelné v produktu IBM MQ for IBM i V5.3 nebo pozdější.

Zahajovací panel se zobrazí na obrázku LU 6.2 -úvodní panel pro nastavení komunikace. Chcete-li získat úplný panel podle obrázku, stiskněte klávesu F10 z prvního panelu.

```
Create Comm Side Information (CRTCSI)
```

```
Type choices, press Enter.
```

```
Side information . . . . . > WINSDOA1   Name
Library . . . . . > QSYS       Name, *CURLIB
Remote location . . . . . > WINSDOA1   Name
Transaction program . . . . . > MQSERIES
```

```
Text 'description' . . . . . *BLANK
```

```
Additional Parameters
```

```
Device . . . . . *LOC       Name, *LOC
Local location . . . . . *LOC       Name, *LOC, *NETATR
Mode . . . . . JSTM092     Name, *NETATR
Remote network identifier . . . *LOC       Name, *LOC, *NETATR, *NONE
Authority . . . . . *LIBCRTAUT Name, *LIBCRTAUT, *CHANGE...
```

```
Bottom
```

```
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

Obrázek 34. Panel inicializace komunikace LU 6.2 -počáteční ukončení

Vyplňte pole iniciace, jak je uvedeno:

Informace o připojení

Zadejte název, který se použije k uložení objektu informací o připojení, který má být vytvořen, například WINSDOA1.

Poznámka: Pro LU 6.2 je to propojení mezi definicí kanálu zpráv a komunikačním připojením pole **Název připojení** definice kanálu zpráv na odesílajícím konci. Toto pole obsahuje název objektu CSI.

Knihovna

Název knihovny, kde je uložena tato definice.

Objekt CSI musí být dostupný v knihovně přístupné pro program obsluhující kanál zpráv, například QSYS, QMQM a QGPL.

Je-li název nesprávný, chybí nebo jej nelze najít, dojde k chybě při spuštění kanálu.

Vzdálené umístění

Uvádí jméno vzdáleného systému, se kterým váš program komunikuje.

Stručně řečeno, tento povinný parametr obsahuje název logické jednotky partnera na vzdáleném systému, jak je definováno v popisu zařízení, které se používá pro komunikační spojení mezi dvěma systémy.

Název **Vzdálený systém** lze nalézt zadáním příkazu DSPNETA na vzdálený systém a zobrazení předvoleného jména lokálního umístění.

Transakční program

Uvádí název (až 64 znaků) transakčního programu na vzdáleném systému, který se má spustit. Může se jednat o název procesu transakce, název programu, název kanálu nebo znakový řetězec, který odpovídá hodnotě **Porovnávací hodnota** v záznamu směrování.

Tento parametr je požadovaný.

Poznámka: Chcete-li zadat názvy transakčních programů služby SNA, zadejte hexadecimální znázornění názvu transakčního programu služby. Chcete-li například zadat název transakčního programu služby s hexadecimální reprezentací 21F0F0F1, zadali byste X'21F0F0F1'.

Další informace o jménech transakčních programů služby SNA najdete v publikaci *SNA Transaction Programmer's Reference* pro LU typu 6.2.

Je-li přijímající konec jiný systém IBM i, použije se název **transakčního programu** k porovnání objektu CSI na odesílajícím konci s položkou směrování na přijímajícím konci. Tento název musí být jedinečný pro každého správce front v cílovém systému IBM i. Viz parametr **Program k volání** pod Initiated end (Receiver). Viz také parametr **comparison data: compare value** na panelu Přidání záznamu směrování.

Textový popis

Popis (až 50 znaků), který vám připomene zamýšlené použití tohoto připojení.

Zařízení

Uvádí jméno popisu zařízení použitého pro vzdálený systém. Možné hodnoty jsou:

* UMÍSTĚNÍ

Zařízení je určeno systémem.

jméno-zařízení

Uvedte jméno zařízení, které je přidruženo ke vzdálenému systému.

Lokální umístění

Uvádí název lokálního umístění. Možné hodnoty jsou:

* UMÍSTĚNÍ

Název lokálního umístění je určen systémem.

* NETATR

Použije se hodnota LCLLOCNAME uvedená v systémových attributech sítě.

Lokální-název-umístění

Uvedte název vašeho umístění. Uvedte lokální umístění, pokud chcete indikovat určité jméno umístění vzdáleného systému. Název umístění lze nalézt pomocí příkazu DSPNETA.

Režim

Uvádí režim používaný pro řízení relace. Tento název je stejný jako u rozhraní CPI (Common Programming Interface)-Communications Mode_Name. Možné hodnoty jsou:

* NETATR

Použije se režim v attributech sítě.

BLANK

Používá se osm prázdných znaků.

Název režimu

Uvedte jméno režimu pro vzdálené umístění.

Poznámka: Vzhledem k tomu, že režim určuje prioritu přenosu komunikační relace, může být užitečné definovat různé režimy v závislosti na prioritě odesílaných zpráv; například MQMODE_HI, MQMODE_MED a MQMODE_LOW. (Můžete mít více než jedno CSI odkazující na stejné umístění.)

Identifikátor vzdálené sítě

Uvádí identifikátor vzdálené sítě použitý se vzdáleným umístěním. Možné hodnoty jsou:

*** UMÍSTĚNÍ**

Použije se ID vzdálené sítě pro vzdálené umístění.

*** NETATR**

Použije se identifikátor vzdálené sítě uvedený v atributech sítě.

*** ŽÁDNÉ**

Vzdálená síť nemá žádný název.

ID-vzdálené-sítě

Uvedte ID vzdálené sítě. Pro vyhledání jména tohoto ID sítě použijte příkaz DSPNETA na vzdáleném umístění. Jedná se o 'ID lokální sítě' ve vzdáleném umístění.

Oprávnění

Uvádí oprávnění, které poskytujete uživatelům, kteří nemají určité oprávnění k objektu, kteří nejsou na seznamu oprávnění, a se skupinovým profilem, který nemá žádné specifické oprávnění k objektu. Možné hodnoty jsou:

*** LIBCRTAUT**

Veřejné oprávnění k objektu je převzato z parametru CRTAUT uvedené knihovny. Tato hodnota se určuje při vytvoření. Změní-li se hodnota parametru CRTAUT pro knihovnu po vytvoření objektu, nová hodnota neovlivní existující objekty.

*** ZMĚNA**

Oprávnění ke změně povoluje uživateli provádět základní funkce na objektu, avšak uživatel nemůže objekt změnit. Oprávnění ke změně poskytuje provozní oprávnění k objektu a oprávnění ke všem datům.

***ALL**

Uživatel může provádět všechny operace kromě těch operací, které jsou omezeny na vlastníka nebo jsou řízeny oprávněním ke správě seznamu oprávnění. Uživatel může řídit existenci objektu a určit zabezpečení objektu, změnit objekt a provádět základní funkce s objektem. Uživatel může měnit vlastnictví objektu.

*** POUŽITÍ**

Oprávnění k použití poskytuje provozní oprávnění k objektu a oprávnění ke čtení.

*** VYLOUČENÍ**

Vyloučit oprávnění zabraňuje uživateli v přístupu k objektu.

Seznam oprávnění

Uvedte jméno seznamu oprávnění s oprávněním, které se používá pro informace o připojení.

Iniciovaný konec (příjímač)

Použijte příkaz CRTMQMCHL, abyste definovali příjímací konec propojení kanálu zpráv s typem přenosu *LU62.

Ponechte pole NÁZEV PŘIPOJENÍ prázdné a ujistěte se, že odpovídající podrobnosti se shodují s odesláním konce kanálu. Podrobnosti naleznete v tématu [Vytvoření kanálu](#).

Chcete-li povolit iniciaci ukončení příjímacího kanálu, přidejte do subsystému na zahájeném konci záznam směrování. Subsystém musí být ten, který alokuje zařízení APPC použité v relacích LU 6.2 . Proto musí mít pro toto zařízení platnou komunikační položku. Směrovací položka volá program, který spouští příjímací konec kanálu zpráv.

Použijte příkazy IBM i (například ADDRTGE) k definování konce odkazu, který je zahájen komunikační relací.

Zahájen koncový panel se zobrazí na panelu nastavení komunikace [LU 6.2 -přidání záznamu směrování](#).

```
Add Routing Entry (ADDRTGE)

Type choices, press Enter.

Subsystem description . . . . . QCMN      Name
Library . . . . . *LIBL      Name, *LIBL, *CURLIB
Routing entry sequence number . 1      1-9999
Comparison data:
Compare value . . . . . MQSERIES

Starting position . . . . . 37      1-80
Program to call . . . . . AMQCRC6B   Name, *RTGDTA
Library . . . . . QMAS400      Name, *LIBL, *CURLIB
Class . . . . . *SBSD      Name, *SBSD
Library . . . . . *LIBL      Name, *LIBL, *CURLIB
Maximum active routing steps . . *NOMAX 0-1000, *NOMAX
Storage pool identifier . . . . . 1      1-10

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

Obrázek 35. Konec komunikačního zařízení LU 6.2 -zahájený konec

Popis podsystému

Název subsystému, ve kterém je umístěna tato definice. Použijte příkaz IBM i WRKSBSD k zobrazení a aktualizaci odpovídajícího popisu podsystému pro směrovací záznam.

Pořadové číslo položky směrování

Jedinečné číslo ve vašem subsystému pro identifikaci této definice komunikace. Můžete použít hodnoty v rozsahu 1-9999.

Porovnávací data: Porovnávací hodnota

Textový řetězec, který se má porovnat s řetězcem přijatým při spuštění relace parametrem **Transaction program**, jak ukazuje [Obrázek 1](#). Znakový řetězec je odvozen z pole Transaction program odesílatele CSI.

Porovnávací údaje: počáteční pozice

Pozice znaku v řetězci, kde má být porovnání spuštěno.

Poznámka: Pole počáteční pozice je pozice znaku v řetězci pro porovnání, a tato pozice je vždy 37.

Program k volání

Název programu, který spouští příchozí program zpráv, který má být volán ke spuštění relace.

Program AMQCRC6A je volán pro výchozího správce front. Tento program je dodáván s produktem IBM MQ for IBM i a nastavuje prostředí a poté volá příkaz AMQCRS6A.

Pro další správce front:

- Každý správce front má specifický program pro vyvolání LU 6.2, který se nachází ve své knihovně. Tento program se nazývá AMQCRC6B a je automaticky generován při vytvoření správce front.
- Každý správce front vyžaduje, aby byla přidána specifická položka směrování s jedinečnými údaji o směrování. Tato data o směrování musí odpovídat názvu **transakčního programu** dodanému žadajícím systémem (viz [Inicializace ukončení \(Sender\)](#)).

Příklad je zobrazen v [konfiguračním panelu komunikace LU 6.2 -zobrazení položek směrování](#):


```

Display Routing Entries
System: MY400
Subsystem description: QCMN      Status: ACTIVE

Type options, press Enter.
5=Display details

Start
Opt  Seq Nbr  Program  Library  Compare Value  Pos
10   *RTGDTA           'QZSCSRVR'      37
20   *RTGDTA           'QZRCRVR'       37
30   *RTGDTA           'QZHQTRG'      37
50   *RTGDTA           'QVPPRINT'     37
60   *RTGDTA           'QNPSRVR'      37
70   *RTGDTA           'QNMAPPINGD'   37
80   QNMAREXECD  QSYS      'AREXECD'       37
90   AMQCRC6A   QMQMBW    'MQSERIES'      37
100  *RTGDTA           'QTFDWNLD'     37
150  *RTGDTA           'QMFRCVR'      37

F3=Exit  F9=Display all detailed descriptions  F12=Cancel

```

Obrázek 36. Konec komunikačního zařízení LU 6.2 -zahájený konec

V okně LU 6.2 communication setup panel-display routing entries, pořadové číslo 90 představuje výchozího správce front a poskytuje kompatibilitu s konfiguracemi z předchozích vydání (tj. V3R2, V3R6, V3R7a V4R2) produktu IBM MQ for IBM i. Tato vydání umožňují pouze jednoho správce front. Pořadová čísla 92 a 94 představují dva další správce front s názvem ALPHA a BETA, které jsou vytvořeny s knihovnami QMALPHA a QMBETA.

Poznámka: Pro každého správce front můžete použít více směrovacích dat pomocí různých směrovacích dat, více než jeden záznam směrování. Tyto záznamy dávají možnost různých priorit práce v závislosti na použitých třídách.

Třída

Název a knihovna třídy použité pro kroky spuštěné prostřednictvím tohoto směrovacího záznamu. Třída definuje atributy běhového prostředí směrovacího kroku a uvádí prioritu úlohy. Musí být uvedena odpovídající položka třídy. Použijte například příkaz WRKCLS k zobrazení existujících tříd nebo pro vytvoření třídy. Další informace o správě pracovních požadavků ze vzdálených logických jednotek LU 6.2 jsou k dispozici v příručce *IBM i Programming: Work Management Guide*.

Poznámka k produktu Work Management

Úloha AMQCRC6A nemůže využít výhod normálních funkcí správy činnosti produktu IBM i, které jsou zdokumentovány v tématu Správa činnosti systému, protože není spuštěna stejným způsobem jako ostatní úlohy produktu IBM MQ. Chcete-li změnit vlastnosti běhového prostředí úloh příjemce LU62, můžete provést jednu z následujících změn:

- Upravte popis třídy uvedený v záznamu směrování pro úlohu AMQCRC6A.
- Změna popisu úlohy v záznamu komunikace

Další informace o konfiguraci komunikačních úloh najdete v příručce *IBM i Programming: Work Management Guide*.

Konfigurace klastru správce front

Klastry poskytují mechanismus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

Než začnete

Úvod do koncepce klastrování najdete v tématu Klastry.

Když navrhujete klastr správců front, musíte provést některá rozhodnutí. Viz [Příklady klastrů](#) a [Navrhování klastrů](#).

Související úlohy

“Přesun definice tématu klastru do jiného správce front” na stránce 336

Pro klastry routed nebo přímé směřované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Související informace

[Odstranit téma](#)

Definování komponent klastru

Klastry se skládají z správců front, kanálů klastru a front klastru. Můžete definovat fronty klastru a upravit některé aspekty výchozích objektů klastru. Můžete získat informace o konfiguraci a stavu o automaticky definovaných kanálech a o vztazích mezi jednotlivými kanály odesílatele klastru a přenosové fronty.

Informace o definování jednotlivých komponent klastru najdete v následujících dílčích tématech:

Související úlohy

“Nastavení nového klastru” na stránce 228

Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

“Přidání správce front do klastru” na stránce 238

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenáší pomocí jedné přenosové fronty klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Související informace

[Komponenty klastru](#)

[Kanály klastru](#)

[Definování témat klastru](#)

Definování front klastru

Fronta klastru je fronta, jejímž hostitelem je správce front klastru, a která je dostupná ostatním správcům front v klastru. Definujte frontu klastru jako lokální frontu ve správci front klastru, kde je fronta hostována. Uveďte název klastru, do kterého fronta patří.

Následující příklad ukazuje příkaz **runmqsc** k definování fronty klastru s volbou CLUSTER :

```
DEFINE QLOCAL(Q1) CLUSTER(SALES)
```

Definice fronty klastru se oznamuje ostatním správcům front v klastru. Ostatní správci front v klastru mohou vkládat zprávy do fronty klastru, aniž by potřebovali odpovídající definici vzdálené fronty. Fronta klastru může být oznámena ve více než jednom klastru pomocí seznamu názvů klastrů.

Po oznámení fronty může každý správce front v klastru do ní vkládat zprávy. Chcete-li správce front vložit zprávu, musí z úplných úložišť zjistit, kdo je hostitelem této fronty. Pak přidá do zprávy informace o směřování a vloží zprávu do přenosové fronty klastru.

 z/OS

Fronta klastru může být fronta, kterou sdílí členové skupiny sdílení front v produktu IBM MQ for z/OS.

Vazba

Můžete vytvořit klastr, ve kterém bude více než jeden správce front hostitelem instance stejné fronty klastru. Ujistěte se, že všechny zprávy v posloupnosti jsou odeslány do stejné instance fronty. Řadu zpráv můžete svázat do konkrétní fronty pomocí volby MQOO_BIND_ON_OPEN na volání MQOPEN .

Přenosové fronty klastru

Správce front může ukládat zprávy pro ostatní správce front z klastru do více přenosových front. Správce front můžete nakonfigurovat tak, aby ukládal zprávy do více přenosových front klastru, dvěma různými způsoby. Když nastavíte atribut správce front **DEFCLXQ** na CHANNEL, vytvoří se jiná přenosová fronta klastru z SYSTEM . CLUSTER . TRANSMIT . MODEL . QUEUE automaticky pro každý odesílací kanál klastru. Pokud nastavíte volbu přenosové fronty CLCHNAME tak, aby se shodovala s jedním nebo více odesílacími kanály klastru, bude správce front moci ukládat zprávy pro odpovídající kanály do těchto přenosových front.



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**.

Zpráva pro frontu klastru v jiném správci front se umístí před odesláním do přenosové fronty klastru. Kanál odesílatele klastru přenáší zprávy z přenosové fronty klastru do kanálů příjemce klastru v jiných správci front. Při výchozím nastavení má jedna systémem definovaná přenosová fronta klastru všechny zprávy, které mají být přeneseny do jiných správců front klastru. Fronta se nazývá SYSTEM . CLUSTER . TRANSMIT . QUEUE. Správce front, který je součástí klastru, může odesílat zprávy na tuto přenosovou frontu klastru libovolnému jinému správci front ve stejném klastru.

Definice pro jednu frontu SYSTEM . CLUSTER . TRANSMIT . QUEUE je standardně vytvářena ve všech správcích správce front kromě z/OS. V systému z/OS může být definice definována s dodaným vzorkem **CSQ4INSX**.

Správce front můžete nakonfigurovat tak, aby přenášels zprávy do jiných klastrovaných správců front používajících více přenosových front. Další přenosové fronty klastru můžete definovat ručně, nebo správce front automaticky vytvořit fronty.

Chcete-li, aby byly fronty vytvořeny automaticky správcem front, změňte atribut správce front DEFCLXQ z SCTQ na CHANNEL. Výsledkem je vytvoření jednotlivé přenosové fronty klastru pro každý odesílací kanál klastru, který je vytvořen. Přenosové fronty jsou vytvářeny jako trvalé dynamické fronty z modelové fronty SYSTEM . CLUSTER . TRANSMIT . MODEL . QUEUE. Název každé trvalé dynamické fronty je SYSTEM . CLUSTER . TRANSMIT . *ChannelName*. Název odesílacího kanálu klastru, ke kterému je přidružena trvalá přenosová fronta dynamického klastru, je nastavena v atributu lokální přenosové fronty CLCHNAME. Zprávy pro vzdálené klastrované správce front se umísťují do trvalé přenosové fronty dynamického klastru pro přidružený odesílací kanál klastru, spíše než na SYSTEM . CLUSTER . TRANSMIT . QUEUE.

Chcete-li vytvořit přenosové fronty klastru ručně, vytvořte lokální frontu s atributem USAGE nastaveným na hodnotu XMITQa atribut CLCHNAME je nastaven na generický název kanálu, který se interpretuje jako jeden nebo více odesílacích kanálů klastru; viz ClusterChannelNázev. Pokud vytvoříte přenosové fronty klastru ručně, máte možnost přidružit přenosovou frontu jedním odesílacím kanálem klastru nebo s více odesílacími kanály klastru. Atribut CLCHNAME je generický název, což znamená, že v názvu můžete umístit více zástupných znaků, "*" .

S výjimkou počátečních odesílacích kanálů klastru, které vytváříte ručně pro připojení správce front k úplnému úložišti, jsou odesílací kanály klastru vytvářeny automaticky. Jsou vytvořeny automaticky, když existuje zpráva pro přenos do správce front klastru. Jsou vytvořeny se stejným názvem jako název přijímacího kanálu klastru, který přijímá zprávy klastru pro tento konkrétní klastr v cílovém správci front.

Pokud postupujete podle konvence pojmenování pro kanály příjemce klastru, je možné definovat generickou hodnotu pro CLCHNAME , která filtruje různé druhy zpráv klastru do různých přenosových front. Pokud například postupujete podle konvence pojmenování pro přijímací kanály klastru produktu *ClusterName . QmgrName*, pak generické jméno *ClusterName . ** filtruje zprávy pro různé klastry v různých přenosových frontách. Musíte definovat přenosové fronty ručně a nastavit CLCHNAME v každé přenosové frontě na *ClusterName . **.

Změny přidružení přenosových front klastru k odesílacím kanálům klastru nepřijímají okamžitý účinek. Momentálně přidružená přenosová fronta, kterou kanál odesílatele klastru obsluhuje, může obsahovat zprávy, které jsou v procesu přenosu kanálem odesílatele klastru. Pouze pokud žádné zprávy v aktuálně

přidružené přenosové frontě nejsou zpracovávány kanálem odesílatele klastru, může správce front změnit přidružení odesílacího kanálu klastru s jinou přenosovou frontou. K tomu může dojít buď v situaci, kdy žádné zprávy nezůstanou v přenosové frontě ke zpracování kanálem odesílatele klastru, nebo když je zpracování zpráv pozastaveno a odesílací kanál klastru nemá žádné zprávy "in-flight". Pokud k tomu dojde, všechny nezpracované zprávy pro kanál odesílatele klastru jsou přeneseny do nově přidružené přenosové fronty a přidružení kanálu odesílatele klastru se změní.

Můžete vytvořit definici vzdálené fronty, která bude interpretována jako přenosová fronta klastru. V definici se správce front QMX nachází ve stejném klastru jako lokální správce front a že neexistuje žádná přenosová fronta, QMX.

```
DEFINE QREMOTE(A) RNAME(B) RQMNAME(QMX)
```

Během rozpoznání názvu fronty má přenosová fronta klastru přednost před výchozí přenosovou frontou. Zpráva umístěná do produktu A je uložena v přenosové frontě klastru a poté odeslána do vzdálené fronty B v systému QMX.

Správci front mohou také komunikovat s ostatními správci front, kteří nejsou součástí klastru. Kanály a přenosové fronty je třeba definovat do druhého správce front stejným způsobem jako v prostředí s rozdělenými frontami.

Poznámka: Aplikace musí zapisovat do front, které se interpretují do přenosové fronty klastru, a nesmí zapisovat přímo do přenosové fronty klastru.

Automatická definice vzdálených front

Správce front v klastru nepotřebuje definici vzdálené fronty pro vzdálené fronty v klastru. Správce front klastru vyhledá umístění vzdálené fronty z úplného úložiště. Přidává informace o směrování do zprávy a vkládá je do přenosové fronty klastru. Produkt IBM MQ automaticky vytvoří definici ekvivalentní definiční definici vzdálené fronty, aby mohla být zpráva odeslána.

Automaticky vytvořenou definici vzdálené fronty nelze změnit ani odstranit. Nicméně pomocí příkazu `DISPLAY QUEUE runmqsc` s atributem `CLUSINFO` můžete zobrazit všechny lokální fronty ve správci front i všechny fronty klastru, včetně front klastru ve vzdálených správcích front. Příklad:

```
DISPLAY QUEUE(*) CLUSINFO
```

Související informace

[Fronty klastru](#)

[Název ClusterChannel\(MQCHAR20\)](#)

Práce s automaticky definovanými kanály odesílatele klastru

Po zavedení správce front do klastru provedením počátečních definic `CLUSSDR` a `CLUSRCVR` produkt IBM MQ při požadavku na přesun zpráv do jiného správce front v klastru automaticky provede další definice kanálů odesílatele klastru. Můžete zobrazit informace o automaticky definovaných odesílacích kanálech klastru, ale nemůžete je upravit. Chcete-li upravit jejich chování, můžete použít uživatelskou proceduru automatické definice kanálu.

Než začnete

Úvod do automaticky definovaných kanálů najdete v tématu [Automaticky definované kanály odesílatele klastru](#).

Informace o této úloze

Automaticky definované kanály odesílatele klastru jsou vytvořeny klastrem jako a v případě potřeby a zůstanou aktivní, dokud nebudou ukončeny pomocí normálních pravidel pro odpojení.

Odesílací kanály klastru (CLUSDR) mohou být automaticky definovány jak pro přesun aplikačních zpráv, tak pro interní administrativní zprávy klastru. Například v klastru Publikování/odběr (jeden ve kterém bylo definováno klastrované téma) lze definovat kanály mezi dílčími úložišti a povolit výměnu stavu 'proxy odběry'. Není-li vyžadováno (neaktivní) po delší dobu, jsou automaticky definované CLUSSDR odebírány z mezipaměti dílčího úložiště informací o klastru a nejsou nadále viditelné pro daného správce front.

Na jiných platformách než z/OS není OAM (správce oprávnění k objektu) informován o existenci automaticky definovaných odesílacích kanálů klastru. Pokud zadáte příkazy **start**, **stop**, **ping**, **reset** nebo **resolve** na automaticky definovaný odesílací kanál klastru, zkontroluje produkt OAM, zda máte oprávnění provádět stejnou akci u odpovídajícího přijímacího kanálu klastru.

z/OS V systému z/OS můžete zabezpečit automaticky definovaný kanál odesílatele klastru stejným způsobem jako kterýkoli jiný kanál.

Procedura

- Zobrazí informace o automaticky definovaných kanálech pro daného správce front klastru.

Pomocí příkazu `DISPLAY CHANNEL runmqsc` nelze zobrazit automaticky definované kanály. Chcete-li zobrazit automaticky definované kanály, použijte následující příkaz:

```
DISPLAY CLUSQMGR(qMgrName)
```

- Zobrazte stav automaticky definovaného kanálu pro danou položku CLUSRCVR.

Chcete-li zobrazit stav automaticky definovaného kanálu CLUSSDR, který odpovídá definici kanálu CLUSRCVR, kterou jste vytvořili, použijte následující příkaz:

```
DISPLAY CHSTATUS(channelName)
```

- Chcete-li upravit chování automaticky definovaného kanálu, použijte proceduru automatické definice kanálu.

Uživatelská procedura automatické definice kanálu produktu IBM MQ můžete použít, chcete-li napsat uživatelský ukončovací program pro přizpůsobení kanálu odesílatele klastru nebo kanálu příjemce klastru. Například můžete použít uživatelskou proceduru pro automatickou definici kanálu v klastrovaném prostředí, abyste provedli libovolnou z následujících úprav:

- Definice komunikačních prostředků, tj. názvy protokolů SNA LU6.2.
- Přidejte nebo odeberte jiné uživatelské procedury, např. uživatelské procedury pro zabezpečení zprávy.
- Změňte názvy uživatelských procedur kanálu.

Název uživatelské procedury kanálu CLUSSDR je automaticky generován z definice kanálu CLUSRCVR, a proto nemusí být vhodný pro vaše potřeby-zejména, pokud jsou dva konce kanálu na různých platformách.

Formát názvů uživatelských procedur se liší na různých platformách. Příklad:

- **z/OS** Na platformě z/OS je formát parametru SCYEXIT (*název uživatelské procedury zabezpečení*) `SCYEXIT('SECEXIT')`.

- **Windows** Na platformách Windows je formát parametru SCYEXIT (*název uživatelské procedury zabezpečení*) `SCYEXIT('drive:\path\library(secexit)')`.

Poznámka: **z/OS** Není-li k dispozici žádná uživatelská procedura automatické definice kanálu, správce front produktu z/OS odvozuje název uživatelské procedury kanálu CLUSSDR z definice kanálu CLUSRCVR na druhém konci kanálu. Chcete-li odvodit název uživatelské procedury z/OS z názvu, který není názvem z/OS, použije se následující algoritmus:

- Názvy uživatelských procedur na platformách jiných než z/OS mají obecný tvar *cesta/knihovna (funkce)*.
- Je-li přítomen *funkce* , použije se až osm znaků.
- Jinak se použije až osm znaků *knihovny* .

Příklad:

- /var/mqm/exits/myExit.so(MsgExit) převádí na MSGEXIT
- /var/mqm/exits/myExit převádí na MYEXIT
- /var/mqm/exits/myExit.so(ExitLongName) převádí na EXITLONG

- Pro správce front starší než IBM MQ verze 7 nastavte atribut **PROPCTL** na hodnotu NONE.

Každý automaticky definovaný kanál odesílatele klastru je založen na příslušném přijímacím kanálu klastru. Před IBM MQ verze 7 nemá kanál příjemce klastru atribut **PROPCTL** , takže tento atribut je proto nastaven na hodnotu COMPAT v automaticky definovaném kanálu odesílatele klastru.

Pokud klastr potřebuje použít produkt **PROPCTL** k odebrání záhlaví aplikací, například RFH2 , ze zpráv, které pochází z produktu IBM MQ verze 7 nebo novější správce front do správce front v dřívější verzi produktu IBM MQ, je nutné zadat uživatelskou proceduru s automatickou definicí kanálu s hodnotou **PROPCTL** na hodnotu NONE.

- Použijte atribut kanálu LOCLADDR. kontrolovat aspekty řešení.
 - Chcete-li povolit odchozí kanál (TCP) pro použití konkrétní adresy IP, portu nebo rozsahu portů, použijte atribut kanálu LOCLADDR. To je užitečné tehdy, máte-li více než jednu síťovou kartu a chcete, aby kanál používal pro odchozí komunikaci určitou specifickou síťovou kartu.
 - Chcete-li určit virtuální adresu IP v kanálu CLUSSDR , použijte adresu IP z LOCLADDR na ručně definovaném CLUSSDR. Chcete-li určit rozsah portů, použijte rozsah portů od CLUSRCVR.
 - Pokud klastr potřebuje použít LOCLADDR k získání odchozích komunikačních kanálů pro připojení k určité adrese IP, můžete zapsat uživatelskou proceduru s automatickou definicí kanálu, aby vynutila hodnotu LOCLADDR do libovolného ze svých automaticky definovaných kanálů CLUSSDR . Je třeba ji zadat také v ručně definovaném kanálu CLUSSDR .
 - Zadejte číslo portu nebo rozsah portů v souboru LOCLADDR kanálu CLUSRCVR , pokud chcete, aby všichni správci front v klastru používali pro všechny své odchozí komunikace specifický port nebo rozsah portů.

Poznámka: Nevkládejte adresu IP do pole LOCLADDR kanálu CLUSRCVR , pokud se všichni správci front nenachází na stejném serveru. Adresa IP LOCLADDR je předána do automaticky definovaných kanálů CLUSSDR všech správců front, které se připojují pomocí kanálu CLUSRCVR .

distributed Na distribuovaných platformách je možné nastavit výchozí hodnotu lokální adresy, která bude použita pro všechny odesílací kanály, pro které není definována lokální adresa. Výchozí hodnota je definována nastavením proměnné prostředí MQ_LCLADDR před spuštěním správce front. Formát hodnoty odpovídá hodnotě atributu MQSC LOCLADDR.

Související informace

[Lokální adresa \(LOCLADDR\)](#)

Práce s výchozími objekty klastru

Výchozí definice kanálů můžete změnit stejným způsobem jako v libovolné jiné definici kanálu spuštěním příkazů MQSC nebo PCF. Neměňte výchozí definice fronty, kromě SYSTEM . CLUSTER . HISTORY . QUEUE.

Úplný seznam těchto objektů najdete v tématu [Výchozí objekty klastru](#). Následující seznam obsahuje pouze ty objekty, které můžete změnit.


SYSTEM . CLUSTER . HISTORY . QUEUE

Každý správce front v klastru má lokální frontu s názvem SYSTEM . CLUSTER . HISTORY . QUEUE.

Produkt SYSTEM . CLUSTER . HISTORY . QUEUE se používá k ukládání historie informací o stavu klastru pro účely služby.

Ve výchozím nastavení objektu je parametr `SYSTEM.CLUSTER.HISTORY.QUEUE` nastaven na hodnotu `PUT (ENABLED)`. Chcete-li potlačit shromažďování historie, změňte nastavení na hodnotu `PUT (DISABLED)`.

SYSTEM.CLUSTER.TRANSMIT.QUEUE

Každý správce front má definici pro lokální frontu s názvem `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. `SYSTEM.CLUSTER.TRANSMIT.QUEUE` je výchozí přenosová fronta pro všechny zprávy do všech front a správců front, kteří jsou v klastrech. Výchozí přenosovou frontu pro každý odesílací kanál klastru můžete změnit na `SYSTEM.CLUSTER.TRANSMIT.ChannelName` změnou atributu správce front `DEFXMITQ` , kromě na `z/OS`. Produkt `SYSTEM.CLUSTER.TRANSMIT.QUEUE` nelze odstranit. Používá se také k definování kontroly autorizace, zda je použita výchozí přenosová fronta, která se používá, `SYSTEM.CLUSTER.TRANSMIT.QUEUE` nebo `SYSTEM.CLUSTER.TRANSMIT.ChannelName`.

Související informace

[Výchozí objekty klastru](#)

Práce s přenosovými frontami klastru a odesílacími kanály klastru

Zprávy mezi správci front s klastru se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru. V libovolném okamžiku je kanál odesílatele klastru asociován s jednou přenosovou frontou. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizováno a transakční.

Spuštěním následujícího příkazu `MQSC` zobrazte přenosové fronty, ke kterým jsou kanály odesílatele klastru přidruženy:

```
DISPLAY CHSTATUS(*) WHERE(CHLTYPE EQ CLUSSDR)
```

```
AMQ8417: Display Channel Status details.  
CHANNEL (TO.QM2)          CHLTYPE (CLUSSDR)  
CONNAME (9.146.163.190(1416))  CURRENT  
RQMNAME (QM2)             STATUS (STOPPED)  
SUBSTATE ( )              XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

Přenosová fronta zobrazená v uloženém stavu kanálu zastaveného kanálu odesílatele klastru se může změnit, jakmile se kanál spustí znovu. [“Výběr výchozích přenosových front podle kanálů odesílatele klastru”](#) na stránce 223 popisuje proces výběru výchozí přenosové fronty; [“Výběr ručně definovaných přenosových front pomocí kanálů odesílatele klastru”](#) na stránce 223 popisuje proces výběru ručně definované přenosové fronty.

Když některý odesílací kanál klastru začne znovu zkontrolovat své přidružení k přenosovým frontám. Pokud se změní konfigurace přenosových front nebo výchozí nastavení správce front, může kanál znovu asociovat s jinou přenosovou frontou. Pokud se kanál restartuje s jinou přenosovou frontou jako výsledek změny konfigurace, provede se proces přenosu zpráv do nově přidružené přenosové fronty. [“Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje”](#) na stránce 224 popisuje proces přenosu odesílacího kanálu klastru z jedné přenosové fronty do jiné.

Chování odesílacích kanálů klastru se liší od kanálů odesílatele a serveru. Zůstávají přidruženy ke stejné přenosové frontě, dokud se nezmění atribut kanálu `XMITQ`. Pokud změňte atribut přenosové fronty na odesílacím kanálu nebo na kanálu serveru a restartujete jej, nebudou zprávy přeneseny z původní přenosové fronty do nové.

Další rozdíl mezi odesílanými kanály klastru a kanály odesílatele nebo serveru znamená, že více odesílacích kanálů klastru může otevřít přenosovou frontu klastru, ale může normální přenosovou frontu otevřít pouze jeden odesílací kanál nebo kanál serveru. Do Verze 7.5 klastrová spojení sdíleli jednu přenosovou frontu klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Počínaje produktem Verze 7.5 máte možnost volby odesílacího kanálu klastru, který nesdílí přenosové fronty. Exkluzivita není vynucena; je výsledkem konfigurace. Cestu ke zprávě lze konfigurovat v klastru tak, aby nesdílela žádné přenosové fronty nebo kanály se zprávami, které tečou mezi ostatními aplikacemi. Viz [Clustering: Planning how to](#)

[configure cluster transmission queues](#) a [“Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány”](#) na stránce 273.

Chcete-li konfigurovat odesílací kanál klastru tak, aby používal jinou přenosovou frontu než `SYSTEM.CLUSTER.TRANSMIT.QUEUE` v systému z/OS je třeba povolit novou funkci verze 8 pomocí režimu operace (`OPMODE`). systémový parametr v makru `CSQ6SYSP`.

Výběr výchozích přenosových front podle kanálů odesílatele klastru

Přenosová fronta klastru je buď systémová předvolená fronta, s názvem, který začíná `SYSTEM.CLUSTER.TRANSMIT`, nebo ručně definovanou frontou. Odesílací kanál klastru je asociován s přenosovou frontou klastru jedním ze dvou způsobů: výchozím mechanismem přenosové fronty klastru nebo ruční konfigurací.

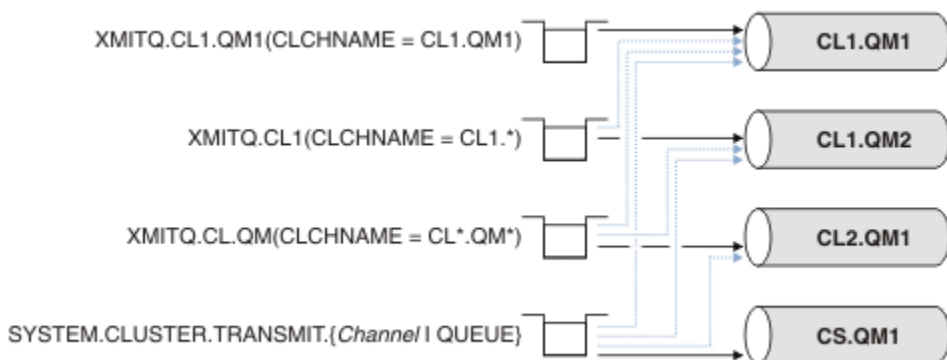
Výchozí přenosová fronta klastru je nastavena jako atribut správce front, **DEFCLXQ**. Jeho hodnota je buď `SCTQ`, nebo `CHANNEL`. Noví a migrovaní správci front jsou nastavovali na hodnotu `SCTQ`. Tuto hodnotu můžete změnit na `CHANNEL`.

Je-li nastavena hodnota `SCTQ`, je výchozí přenosová fronta klastru `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Tuto frontu může otevřít každý odesílací kanál klastru. Odesílací kanály klastru, které otvírají frontu, jsou ty, které nejsou přidruženy k ručně definovaným přenosovým frontám klastru.

Je-li nastavena volba `CHANNEL`, může správce front vytvořit samostatnou trvalou dynamickou přenosovou frontu pro každý odesílací kanál klastru. Každá fronta má název `SYSTEM.CLUSTER.TRANSMIT.ChannelName` a je vytvořena z modelové fronty `SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE`. Každý odesílací kanál klastru, který není přidružen k ručně definované přenosové frontě klastru, je přidružen k frontě pro přenosovou frontu trvalého dynamického klastru. Fronta je vytvořena správcem front, vyžaduje-li pro cíl klastru obsluhovaný tímto odesílacím kanálem klastru samostatnou přenosovou frontu klastru a žádná fronta neexistuje.

Některá místa určení klastru mohou být obsluhována odesílacími kanály klastru přidruženými k ručně definovaným frontám přenosu a ostatním prostřednictvím výchozí fronty nebo front. V přidružení odesílacích kanálů klastru s přenosovými frontami mají ručně definované přenosové fronty vždy přednost před výchozími přenosovými frontami.

Pořadí přenosových front klastru je ilustrováno v [Obrázek 37](#) na stránce 223. Jediný odesílací kanál klastru, který není přidružený k ručně definované přenosové frontě klastru, je `CS.QM1`. Nevztahuje se k ručně definované přenosové frontě, protože žádný z názvů kanálů v atributu **CLCHNAME** přenosových front neodpovídá `CS.QM1`.



Obrázek 37. Priorita přenosové fronty/klastru-priorita odesílatele

Výběr ručně definovaných přenosových front pomocí kanálů odesílatele klastru

Ručně definovaná fronta má atribut **USAGE** atributu přenosové fronty nastavený na hodnotu `XMITQa` atribut názvu kanálu klastru **CLCHNAME** je nastaven na specifický nebo generický název kanálu.

Pokud se název v atributu fronty produktu **CLCHNAME** shoduje s názvem kanálu odesílatele klastru, kanál je přidružen ke frontě. Název je buď přesná shoda, pokud název neobsahuje žádné zástupné znaky, nebo to nejlepší shodu, pokud název obsahuje zástupné znaky.

Pokud se definice **CLCHNAME** ve více přenosových frontách shodují se stejným kanálem odesílatele klastru, definice se mají překrývat. Chcete-li vyřešit nejednoznačnost, existuje pořadí priorit mezi shodami. Přesná shoda má vždy přednost. Obrázek 37 na stránce 223 zobrazuje přidružení mezi přenosovou frontou a odesílacími kanály klastru. Černé šipky ukazují skutečné svazy a šedé šipky, potenciální svazy. Pořadí priorit přenosových front v produktu Obrázek 37 na stránce 223 je následující:

XMITQ.CL1.QM1

Přenosová fronta XMITQ.CL1.QM1 má svůj atribut **CLCHNAME** nastaven na CL1.QM1. Definice atributu **CLCHNAME**, CL1.QM1, nemá žádné zástupné znaky a má přednost před všemi ostatními atributy CLCHNAME definovanými v jiných přenosových frontách, které se shodují se zástupnými znaky. Správce front uloží jakoukoli zprávu klastru, která má být přenesena kanálem odesílatele klastru CL1.QM1 do přenosové fronty produktu XMITQ.CL1.QM1. Jediná výjimka je, pokud má více přenosových front svůj atribut **CLCHNAME** nastaven na CL1.QM1. V takovém případě správce front ukládá zprávy pro odesílací kanál klastru CL1.QM1 v jakékoli z těchto front. Vybírá frontu libovolně, když se spustí kanál. Je-li kanál znovu spuštěn, může být vybrána jiná fronta.

XMITQ.CL1

Přenosová fronta XMITQ.CL1 má svůj atribut **CLCHNAME** nastaven na CL1.*. Definice atributu **CLCHNAME**, CL1.*, má jeden koncový zástupný znak, který odpovídá názvu libovolného kanálu odesílatele klastru, který začíná na CL1.. Správce front uloží všechny zprávy klastru, které mají být přeneseny libovolným odesílacím kanálem klastru, jehož název začíná na CL1. v přenosové frontě XMITQ.CL1, pokud neexistuje přenosová fronta se specifičtější shodou, jako je fronta XMITQ.CL1.QM1. Jeden koncový zástupný znak učiní definici méně specifickou než definici bez zástupných znaků a specifičtější než definice s více zástupnými znaky, nebo zástupné znaky, za kterými následují další koncové znaky.

XMITQ.CL.QM

XMITQ.CL.QM je název přenosové fronty se svým atributem **CLCHNAME** nastaveným na CL*.QM*. Definice produktu CL*.QM* má dva zástupné znaky, které se shodují s názvem kanálu odesílatele klastru, který začíná na CL., a to buď zahrnuje, nebo končí na QM. Shoda je méně specifická než shoda s jedním zástupným znakem.

SYSTEM.CLUSTER.TRANSMIT.channelName |QUEUE

Pokud nemá žádná přenosová fronta atribut **CLCHNAME**, který odpovídá názvu kanálu odesílatele klastru, který má být používán správcem front, pak správce front použije výchozí přenosovou frontu klastru. Výchozí přenosová fronta klastru je buď přenosová fronta klastru jednoho systému, SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo přenosová fronta klastru systému, kterou správce front vytvořil pro specifický odesílací kanál klastru, SYSTEM.CLUSTER.TRANSMIT.channelName. Která fronta je výchozí, závisí na nastavení atributu správce front **DEFXMITQ**.

Tip: Pokud nemáte jasnou potřebu překrývajících se definic, vyhněte se jim, protože mohou vést ke složitým konfiguracím, které jsou těžko pochopitelné.

Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje

Chcete-li změnit přidružení odesílacích kanálů klastru ke frontám přenosu klastru, změňte parametr **CLCHNAME** v libovolné přenosové frontě nebo parametru správce front **DEFCLXQ** kdykoli. Nic se nestane okamžitě. Změny se vyskytnou pouze při spuštění kanálu. Když se spustí, bude kontrolovat, zda pokračovat ve směrování zpráv ze stejné přenosové fronty. Tři druhy změn mění přidružení odesílacího kanálu klastru k přenosové frontě.

1. Při předefinování parametru **CLCHNAME** přenosové fronty je kanál odesílatele klastru v současné době přidružen k méně specifickému nebo mezerovému stavu, nebo při zastavení kanálu se odstraní přenosové fronty klastru.

Pro název kanálu by nyní mohla být lepší shoda s jinou přenosovou frontou klastru. Nebo, pokud se žádné jiné přenosové fronty neshodují s názvem kanálu odesílatele klastru, přidružení se musí vrátit k výchozí přenosové frontě.

2. Předefinování parametru **CLCHNAME** jakékoli jiné přenosové fronty klastru nebo přidání přenosové fronty klastru.

Parametr **CLCHNAME** jiné přenosové fronty může nyní být lepší pro kanál odesílatele klastru, než je odesílací kanál, se kterým je aktuálně asociován odesílací kanál klastru. Je-li odesílací kanál klastru momentálně přidružen k výchozí přenosové frontě klastru, může být přidružen k ručně definované přenosové frontě klastru.

3. Je-li odesílací kanál klastru aktuálně přidružen k výchozí přenosové frontě klastru, změňte parametr správce front **DEFCLXQ**.

Změní-li se přidružení odesílacího kanálu klastru, změní-li se kanál, přepne se do nové přenosové fronty. Během přepínače se ujistí, že žádné zprávy nejsou ztraceny. Zprávy se přenášejí do nové přenosové fronty v pořadí, ve kterém bude kanál přenášet zprávy do vzdáleného správce front.

Zapamatujte si: Při předávání zpráv v klastru je třeba do skupin vložit zprávy, které zajistí, že zprávy, které musí být doručovány v pořadí, jsou doručovány v pořadí. Ve výjimečných případech může dojít k nedostatku zpráv v klastru.

Proces přepnutí probíhá přes následující transakční kroky. Je-li proces přepnutí přerušeno, aktuální transakční krok se obnoví znovu, když se kanál znovu spustí.

Krok 1-Zpracování zpráv z původní přenosové fronty

Odesílací kanál klastru je přidružen k nové přenosové frontě, kterou může sdílet s ostatními odesílacími kanály klastru. Zprávy pro kanál odesílatele klastru budou nadále umístěny do původní přenosové fronty. Přejídný proces přepnutí přenesou zprávy z původní přenosové fronty do nové přenosové fronty. Odesílací kanál klastru předává zprávy z nové přenosové fronty do přijímacího kanálu klastru. Stav kanálu ukazuje odesílací kanál klastru, který je stále přidružen ke staré přenosové frontě.

Proces přepnutí také pokračuje v přenášení nově příchozích zpráv. Tento krok pokračuje, dokud počet zbývajících zpráv, které se mají postoupit procesem přepnutí, dosáhne nulové hodnoty. Když počet zpráv dosáhne nuly, procedura se přesune na krok 2.

Během kroku 1 se zvyšuje aktivita disku pro kanál. Trvalé zprávy jsou potvrzeny z první přenosové fronty a do druhé přenosové fronty. Tato disková aktivita je navíc k potvrzeným zprávám, když jsou umístěny do přenosové fronty a odstraněny z přenosové fronty jako součást přenosu zpráv normálně. V ideálním případě se během procesu přepínání nepřijímají žádné zprávy, takže přechod se může uskutečnit co nejrychleji. Pokud zprávy dorazí, zpracují se procesem přepnutí.

Krok 2-Zpracovat zprávy z nové přenosové fronty

Jakmile žádné zprávy zůstanou v původní přenosové frontě pro odesílací kanál klastru, budou nové zprávy umístěny přímo do nové přenosové fronty. Stav kanálu ukazuje, že kanál odesílatele klastru je přidružen k nové přenosové frontě. Do protokolu chyby správce front se zapíše následující zpráva: "AMQ7341 Přenosová fronta pro kanál *ChannelName* je *QueueName*."

Více přenosových front klastru a atributů přenosové fronty klastru

Máte možnost volby postoupení zpráv klastru různým správcům front, které ukládají zprávy do jedné přenosové fronty klastru nebo do více front. S jednou frontou máte jednu sadu atributů přenosové fronty klastru k nastavení a dotazu; s více frontami máte více sad. Pro některé atributy je výhodou více sad: například dotaz na hloubku fronty informuje o tom, kolik zpráv čeká na postoupení prostřednictvím jedné nebo více kanálů, nikoli všemi kanály. Pro další atributy je v nevýhodě více sad: například pravděpodobně nechcete konfigurovat stejná přístupová oprávnění pro každou přenosovou frontu klastru. Z tohoto důvodu jsou přístupová oprávnění vždy kontrolována proti profilu pro produkt `SYSTEM.CLUSTER.TRANSMIT.QUEUE` a nikoli pro profily pro konkrétní přenosovou frontu klastru. Chcete-li aplikovat podrobnější kontroly zabezpečení, prostudujte si téma [Řízení přístupu a více přenosových front klastru](#).

Více odesílacích kanálů klastru a více přenosových front

Správce front uloží zprávu do přenosové fronty klastru před tím, než ji předá na odesílací kanál klastru. Vybere kanál odesílatele klastru, který je připojen k místu určení pro zprávu. Může jít o výběr

odesílacích kanálů klastru, které se všechny připojují ke stejnému cíli. Místo určení může být stejná fyzická fronta připojená více odesílacími kanály klastru k jednomu správci front. Místo určení může být také mnoho fyzických front se stejným názvem fronty, které jsou hostované na různých správcích front ve stejném klastru. Pokud existuje volba kanálů odesílatele klastru připojených k místu určení, algoritmus vyrovnávání pracovní zátěže si zvolí jeden z nich. Volba závisí na řadě faktorů. Další informace naleznete v tématu [Algoritmus správy pracovní zátěže klastru](#).

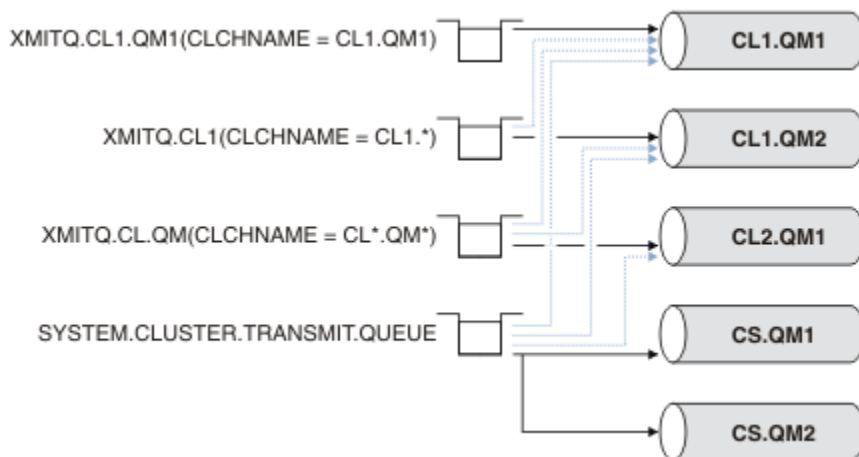
V systémech [Obrázek 38](#) na stránce 227, CL1.QM1, CL1.QM2 a CS.QM1 jsou všechny kanály, které mohou vést ke stejnému cíli. Pokud například definujete Q1 v CL1 na QM1 a QM2 pak CL1.QM1 a CL1.QM2 obě poskytují přenosové cesty ke stejnému cíli, Q1, na dvou různých správcích front. Je-li kanál CS.QM1 také v CL1, je to také kanál, který může přijmout zpráva pro Q1. Členství v klastru produktu CS.QM1 může být definováno v seznamu názvů klastru, což je důvod, proč název kanálu neobsahuje v jeho konstrukci název klastru. V závislosti na parametrech vyrovnávání pracovní zátěže a v odesílající aplikaci mohou být některé zprávy pro Q1 umístěny na každou přenosovou frontu, XMITQ.CL1.QM1, XMITQ.CL1 a SYSTEM.CLUSTER.TRANSMIT.CS.QM1.

Pokud chcete oddělit provoz zpráv, takže zprávy pro stejné místo určení nesdílejí fronty nebo kanály se zprávami pro různá místa určení, musíte nejprve zvážit, jak rozdělit provoz na různé odesílací kanály klastru, a pak jak oddělit zprávy pro konkrétní kanál do jiné přenosové fronty. Klastrované fronty ve stejném klastru, ve stejném správci front, obvykle sdílejí stejné kanály klastru. Definování více přenosových front klastru samo o sobě nepostačuje k oddělení provozu zpráv klastru do různých front. Pokud neoddělíte zprávy pro různé cílové fronty na různých kanálech, budou zprávy sdílet stejnou přenosovou frontu klastru.

Přímočarým způsobem, jak oddělit kanály, které zprávy přijímají, je vytvořit více klastrů. V každém správci front v každém klastru definujte pouze jednu frontu klastru. Definujete-li pro každou kombinaci klastru a správce front jiný kanál příjemce klastru, zprávy pro každou frontu klastru nesdílejí kanál klastru se zprávami pro jiné fronty klastru. Definujete-li oddělené přenosové fronty pro kanály klastru, odesílající správce front ukládá zprávy pouze pro jednu frontu klastru v každé přenosové frontě. Pokud například chcete, aby dvě fronty klastru nesdílely prostředky, můžete je buď umístit do různých klastrů ve stejném správci front, nebo na různých správcích front ve stejném klastru.

Volba přenosové fronty klastru nemá vliv na algoritmus vyrovnávání pracovní zátěže. Algoritmus vyrovnávání pracovní zátěže si vybírá, který kanál odesílatele klastru má předat zprávu. Zpráva umístí zprávu do přenosové fronty, která je obsluhována daným kanálem. Je-li pro algoritmus vyrovnávání pracovní zátěže volán znovu, například pokud se kanál zastaví, může být schopen vybrat jiný kanál k předání zprávy. Pokud si zvolí jiný kanál a nový kanál předává zprávy z jiné přenosové fronty klastru, algoritmus vyrovnávání pracovní zátěže přenesení zprávu do jiné přenosové fronty.

V produktu [Obrázek 38](#) na stránce 227 jsou k výchozí přenosové frontě systému přidruženy dva kanály odesílatele klastru CS.QM1 a CS.QM2. Když algoritmus vyrovnávání pracovní zátěže ukládá zprávu v produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE nebo v jiné přenosové frontě klastru, je název odesílacího kanálu klastru, který má předat zprávu, uložen do ID korelace zprávy. Každý kanál předává pouze ty zprávy, které odpovídají ID korelace s názvem kanálu.



Obrázek 38. Více odesílacích kanálů klastru

Pokud se produkt CS.QM1 zastaví, budou prozkoumány zprávy v přenosové frontě pro daný odesílací kanál klastru. Tyto zprávy, které mohou být předány jiným kanálem, jsou znovu zpracovány algoritmem vyrovnávání pracovní zátěže. Jejich ID korelace je resetováno na alternativní název kanálu odesílatele klastru. Je-li alternativní odesílací kanál klastru CS.QM2, zpráva zůstane na SYSTEM.CLUSTER.TRANSMIT.QUEUE. Je-li alternativní kanál CL1.QM1, algoritmus vyrovnávání pracovní zátěže přenesou zprávu do produktu XMITQ.CL1.QM1. Jsou-li restartována odesílací kanál klastru, nové zprávy a zprávy, které nebyly označeny příznakem pro jiný odesílací kanál klastru, jsou znovu přeneseny kanálem.

Přidružení mezi přenosovými frontami a odesílacími kanály klastru můžete změnit na spuštěném systému. V přenosové frontě můžete změnit parametr CLCHNAME nebo změnit parametr správce front **DEFCLXQ**. Když se kanál, který je ovlivněn změnou restartů, spustí proces přepínání přenosové fronty, viz [“Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje”](#) na stránce 224.

Proces přepnutí přenosové fronty se spustí, když se kanál restartuje. Proces vyvažování zátěže se spustí po zastavení kanálu. Tyto dva procesy mohou běžet paralelně.

Jednoduchý případ při zastavení kanálu odesílatele klastru nezpůsobí, že proces nového vyvažování klastru změní kanál odesílatele klastru, který má předat zprávy ve frontě. Tento případ se týká případu, kdy žádný jiný odesílací kanál klastru nemůže předat zprávy do správného místa určení. Pokud neexistuje alternativní odesílací kanál klastru k předání zpráv do místa určení, zprávy zůstanou pro stejný odesílací kanál klastru po zastavení kanálu odesílatele klastru označeny příznakem pro stejný kanál odesílatele klastru. Když se kanál spustí, pokud je přepínač v nevyřízeném stavu, přesune tyto zprávy do jiné přenosové fronty, kde jsou zpracovávány stejným odesílacím kanálem klastru.

Složenější případ je místo, kde více než jeden odesílací kanál klastru může zpracovávat některé zprávy do stejného cíle. Chcete-li aktivovat přepínač přenosové fronty, zastavte a znovu spusťte odesílací kanál klastru. V mnoha případech při restartování kanálu již algoritmus vyrovnávání pracovní zátěže přesunul zprávy z původní přenosové fronty do různých přenosových front obsluhovaných různými kanály odesílatele klastru. Do nové přenosové fronty zůstanou přeneseny pouze ty zprávy, které nelze předat jiným odesílacím kanálem klastru. V některých případech, je-li kanál restartován rychle, zůstávají některé zprávy, které mohou být přeneseny algoritmem vyrovnávání pracovní zátěže. V takovém případě jsou některé zbývající zprávy přepnuty procesem vyrovnávání pracovní zátěže a některým procesem přepnutí přenosové fronty.

Související pojmy

[“Výpočet velikosti protokolu”](#) na stránce 463

[Odhadování velikosti protokolu, které správce front potřebuje.](#)

Související úlohy

[“Vytvoření dvou překrývajících se klastrů se správcem front brány”](#) na stránce 263

Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv do jedné aplikace ze zpráv do jiných aplikací v klastru.

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 240

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

“Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 270

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

“Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 273

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

Související informace

Kanály klastru

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

Nastavení nového klastru

Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

Než začnete

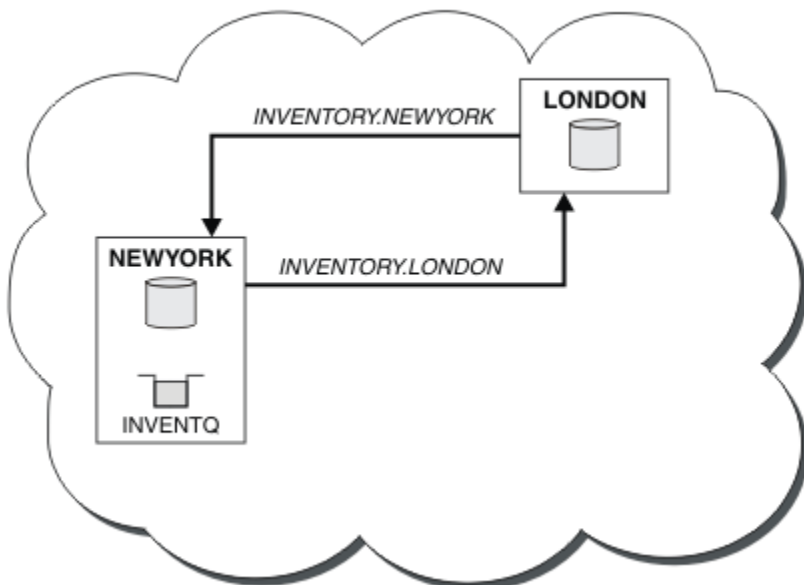
- Místo následujících pokynů můžete pomocí jednoho z průvodců dodávaných s produktem MQ Explorer vytvořit klastr podobný tomu, který vytvořil tato úloha. Klepněte pravým tlačítkem myši na složku **Klastry správců front** a poté klepněte na volbu **Nový > Klastr správců fronta** postupujte podle pokynů uvedených v průvodci.
- Doplnující informace týkající se podpory pokynů k nastavení klastru najdete v tématu “Definování front klastru” na stránce 217, Kanály klastru a Listenery.

Informace o této úloze

Nastavujete novou síť IBM MQ pro úložiště řetězců. Obchod má dvě pobočky, jeden v Londýně a jeden v New Yorku. Data a aplikace pro každé úložiště jsou hostovány systémy, které spouštějí samostatné správce front. Dva správci front se nazývají LONDON a NEWYORK. Aplikace soupisu se spustí na systému v New Yorku, který je připojen ke správci front NEWYORK. Aplikace je řízena doručením zpráv ve frontě INVENTQ hostované serverem NEWYORK. Dva správci front, LONDON a NEWYORK, mají být propojeny v klastru s názvem INVENTORY, takže mohou oba vkládat zprávy do INVENTQ.

Obrázek 39 na stránce 229 ukazuje, jak tento klastr vypadá.

INVENTORY



Obrázek 39. Klastř INVENTORY se dvěma správci front

Každý správce front v klastř můžete nakonfigurovat tak, aby odesílal zprávy jiným správčům front v klastř pomocí různých přenosových front klastř.

Pokyny pro nastavení klastř se liší podle transportního protokolu, počtu přenosových front nebo platformy. Máte na výběr ze tří kombinací. Ověřovací procedura zůstane stejná pro všechny kombinace.

Procedura

- [“Nastavení klastř pomocí protokolu TCP/IP s jedinou přenosovou frontou na správce front” na stránce 230](#)
- [“Nastavení klastř v systému TCP/IP s použitím více přenosových front na jednoho správce front” na stránce 232](#)
- [“Nastavení klastř pomocí LU 6.2 na systému z/OS” na stránce 235](#)
- [“Ověření klastř” na stránce 237](#)

Výsledky

Obrázek 39 na stránce 229 zobrazuje nastavení klastř INVENTORY pomocí této úlohy.

Je zřejmé, že INVENTORY je malý klastř. Nicméně je to užitečné jako důkaz konceptu. Důležitým krokem při pochopení tohoto klastř je rozsah, který nabízí pro budoucí vylepšení.

Související úlohy

[“Konfigurace klastř správce front” na stránce 216](#)

Klastř poskytují mechanismus pro propojení správčů front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastř a vytvářet a spravovat klastř.

Související informace

[Klastř](#)

[Porovnání klastřování a distribuovaných front](#)


[Komponenty klastř](#)

Nastavení klastru pomocí protokolu TCP/IP s jedinou přenosovou frontou na správce front

Než začnete

- Atribut správce front, **DEFCLXQ**, musí být ponechán jako výchozí hodnota SCTQ.

Informace o této úloze

Chcete-li nastavit klastr v systému AIX, HP-UX, IBM i, Linux, Solaris a Okna pomocí protokolu přenosu TCP/IP, postupujte takto.  V systému z/OSmusíte postupovat podle pokynů v části “Definování připojení TCP na systému z/OS” na stránce 611 , chcete-li nastavit připojení TCP/IP, spíše než definovat listenery v kroku “4” na stránce 231. Jinak jsou kroky stejné pro produkt z/OS, ale chybové zprávy se zapisují na konzolu a nikoli do protokolu chyb správce front.

Postup

1. Rozhodněte se pro organizaci klastru a jeho název.

Rozhodli jste se propojit dva správce front, LONDON a NEWYORK, do klastru. Klastr s pouze dvěma správci front nabízí pouze okrajovou výhodu v rámci sítě, která má používat distribuované řazení do fronty. Je to dobrý způsob, jak začít, a poskytuje prostor pro budoucí expanzi. Když otevřete nové větve svého úložiště, můžete do klastru snadno přidávat nové správce front. Přidání nových správců front nenaruší existující síť; viz “Přidání správce front do klastru” na stránce 238.

Prozatím se jedná o jedinou aplikaci, kterou spouštíte, je aplikace inventarizace. Název klastru je INVENTORY.

2. Rozhodněte se, které správci front mají uchovávat úplná úložiště.

V každém klastru musíte navrhnout alespoň jednoho správce front, nebo nejlépe dva, aby se udržela úplná úložiště. V tomto příkladu jsou pouze dva správci front, LONDON a NEWYORK, z nichž obě zadržují úplná úložiště.

- a. Zbývající kroky můžete provést v libovolném pořadí.
- b. Během kroků se mohou do protokolu správce front zapisovat varovné zprávy. Zprávy jsou výsledkem chybějících definic, které jste ještě přidali.

Examples of the responses to the commands are shown in a box like this after each step in this task. These examples show the responses returned by IBM MQ for AIX. The responses vary on other platforms.

- c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštěni správci front.

3. Upravte definice správce front tak, aby byly přidány definice úložiště.

V každém správci front, který má uchovávat úplné úložiště, změňte definici lokální správce front pomocí příkazu ALTER QMGR a zadáním atributu REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: Websphere MQ queue manager changed.
```

Zadáte-li například:

- a. runmqsc LONDON
- b. ALTER QMGR REPOS(INVENTORY)

LONDON se změní na úplné úložiště.

4. Definujte moduly listener.

Definujte modul listener, který přijímá požadavky na síť od ostatních správců front pro každého správce front v klastru. Na správcích front produktu LONDON zadejte následující příkaz:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
```

Atribut CONTROL zajišťuje, že se modul listener spustí a zastaví v okamžiku, kdy správce front ano.

Listener není spuštěn, když je definován, takže musí být ručně spuštěn poprvé s následujícím příkazem MQSC:

```
START LISTENER(LONDON_LS)
```

Vydejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každou z nich.

Existuje několik způsobů, jak tyto listenery definovat, jak je zobrazeno v [Listenerech](#).

5. Definujte kanál CLUSRCVR pro správce front LONDON .

V každém správci front v klastru můžete definovat kanál příjemce klastru, v němž může správce front přijímat zprávy. Viz [Channel-receiver channel: CLUSRCVR](#) . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, na které se mohou odkazovat další správci front. Klíčové slovo CLUSTER zobrazuje dostupnost správce front pro příjem zpráv od jiných správců front v klastru.

V tomto příkladu je název kanálu INVENTORY . LONDONa název připojení (CONNAME) je síťová adresa počítače, kde se nachází správce front, což je LONDON . CHSTORE . COM. Adresu sítě lze zadat jako alfanumerický název hostitele DNS nebo adresu IP ve tečkové desítkové tečkové notaci IPv4 . Příklad: 192 . 0 . 2 . 0nebo hexadecimální tvar IPv6 ; například 2001 : DB8 : 0204 : acff : fe97 : 2c34 : fde0 : 3485. Číslo portu není uvedeno, takže se použije výchozí port (1414).

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
AMQ8014: Websphere MQ channel created.
07/09/98 12:56:35 No repositories for cluster 'INVENTORY'
```

6. Definujte kanál CLUSRCVR pro správce front NEWYORK .

Pokud modul listener kanálu používá výchozí port, obvykle 1414, a klastr neobsahuje správce front v produktu z/OS, můžete parametr CONNAME vynechat.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
```

7. Definujte kanál CLUSSDR na správci front LONDON .

Kanál CLUSSDR můžete ručně definovat ze všech správců front úplného úložiště do všech ostatních správců front úplného úložiště v klastru. Viz [Odesílací kanál klastru: CLUSSDR](#) . V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který ukazuje na kanál CLUSRCVR definovaný v jiném správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Má-li správce front definice pro kanál příjemce klastru a odesílací kanál klastru ve stejném klastru, bude kanál odesílatele klastru spuštěn.


```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: Websphere MQ channel created.
07/09/98 13:00:18 Channel program started.
```

8. Definujte kanál CLUSSDR na správci front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from NEWYORK to repository at LONDON')
```

9. Definujte frontu klastru INVENTQ

Definujte frontu INVENTQ ve správci front NEWYORK zadáním klíčového slova CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: Websphere MQ queue created.
```

Klíčové slovo CLUSTER způsobí, že fronta bude inzerována do klastru. Jakmile je fronta definována, bude zpřístupněna pro ostatní správce front v klastru. Mohou do ní odesílat zprávy, aniž by bylo nutné pro ni vytvořit definici vzdálené fronty.

Všechny definice jsou dokončené. Na všech platformách spusťte program modulu listener na každém správci front. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

Nastavení klastru v systému TCP/IP s použitím více přenosových front na jednoho správce front

Informace o této úloze

Chcete-li nastavit klastr v systému AIX, HP-UX, IBM i, Linux, Solaris a Okna pomocí protokolu přenosu TCP/IP, postupujte takto. Správci front úložiště jsou konfigurováni pro použití jiné přenosové fronty klastru k odesílání zpráv mezi sebou a ostatním správčům front v klastru. Přidáte-li do klastru správce front, který má také používat různé přenosové fronty, postupujte podle úlohy [“Přidání správce front do klastru: samostatné přenosové fronty”](#) na stránce 240.

Postup

1. Rozhodněte se pro organizaci klastru a jeho název.

Rozhodli jste se propojit dva správce front, LONDON a NEWYORK, do klastru. Klastr s pouze dvěma správci front nabízí pouze okrajovou výhodu v rámci sítě, která má používat distribuované řazení do fronty. Je to dobrý způsob, jak začít, a poskytuje prostor pro budoucí expanzi. Když otevřete nové větve svého úložiště, můžete do klastru snadno přidávat nové správce front. Přidání nových správců front nenaruší existující síť; viz [“Přidání správce front do klastru”](#) na stránce 238.

Prozatím se jedná o jedinou aplikaci, kterou spouštíte, je aplikace inventarizace. Název klastru je INVENTORY.

2. Rozhodněte se, které správce front mají uchovávat úplná úložiště.

V každém klastru musíte navrhnout alespoň jednoho správce front, nebo nejlépe dva, aby se udržela úplná úložiště. V tomto příkladu jsou pouze dva správci front, LONDON a NEWYORK, z nichž obě zadržují úplná úložiště.

- a. Zbývající kroky můžete provést v libovolném pořadí.
- b. Během kroků se mohou do protokolu správce front zapisovat varovné zprávy. Zprávy jsou výsledkem chybějících definic, které jste ještě přidali.

```
Examples of the responses to the commands are shown in a box
like this after each step in this task.
These examples show the responses returned by IBM MQ for AIX.
The responses vary on other platforms.
```

- c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštěni správci front.
3. Upravte definice správce front tak, aby byly přidány definice úložiště.

V každém správci front, který má uchovávat úplné úložiště, změňte definici lokální správce front pomocí příkazu ALTER QMGR a zadáním atributu REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: Websphere MQ queue manager changed.
```

Zadáte-li například:

- a. runmqsc LONDON
- b. ALTER QMGR REPOS(INVENTORY)

LONDON se změní na úplné úložiště.

4. Upravte definice správce front tak, aby vytvořily samostatné přenosové fronty klastru pro každý cíl.

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

U každého správce front, kterého jste přidali do klastru, se rozhodněte, zda chcete použít samostatné přenosové fronty nebo ne. Viz témata [“Přidání správce front do klastru”](#) na stránce 238 a [“Přidání správce front do klastru: samostatné přenosové fronty”](#) na stránce 240.

5. Definujte moduly listener.

Definujte modul listener, který přijímá požadavky na síť od ostatních správců front pro každého správce front v klastru. Na správcích front produktu LONDON zadejte následující příkaz:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
```

Atribut CONTROL zajišťuje, že se modul listener spustí a zastaví v okamžiku, kdy správce front ano.

Listener není spuštěn, když je definován, takže musí být ručně spuštěn poprvé s následujícím příkazem MQSC:

```
START LISTENER(LONDON_LS)
```

Vydejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každou z nich.

Existuje několik způsobů, jak tyto listenery definovat, jak je zobrazeno v [Listenerech](#).

6. Definujte kanál CLUSRCVR pro správce front LONDON .

V každém správci front v klastru můžete definovat kanál příjemce klastru, v němž může správce front přijímat zprávy. Viz [Channel-receiver channel: CLUSRCVR](#) . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, na které se mohou odkazovat další správci front. Klíčové slovo CLUSTER zobrazuje dostupnost správce front pro příjem zpráv od jiných správců front v klastru.

V tomto příkladu je název kanálu INVENTORY . LONDON a název připojení (CONNAME) je síťová adresa počítače, kde se nachází správce front, což je LONDON . CHSTORE . COM. Adresu sítě lze zadat jako alfanumerický název hostitele DNS nebo adresu IP ve tečkové desítkové tečkové notaci IPv4 . Příklad: 192 . 0 . 2 . 0 nebo hexadecimální tvar IPv6 ; například 2001 : DB8 : 0204 : acff : fe97 : 2c34 : fde0 : 3485. Číslo portu není uvedeno, takže se použije výchozí port (1414).

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
AMQ8014: Websphere MQ channel created.
07/09/98 12:56:35 No repositories for cluster 'INVENTORY'
```

7. Definujte kanál CLUSRCVR pro správce front NEWYORK .

Pokud modul listener kanálu používá výchozí port, obvykle 1414, a klastr neobsahuje správce front v produktu z/OS, můžete parametr CONNAME vynechat.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
```

8. Definujte kanál CLUSSDR na správci front LONDON .

Kanál CLUSSDR můžete ručně definovat ze všech správců front úplného úložiště do všech ostatních správců front úplného úložiště v klastru. Viz [Odesílací kanál klastru: CLUSSDR](#) . V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který ukazuje na kanál CLUSRCVR definovaný v jiném správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Má-li správce front definice pro kanál příjemce klastru a odesílací kanál klastru ve stejném klastru, bude kanál odesílatele klastru spuštěn.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: Websphere MQ channel created.
07/09/98 13:00:18 Channel program started.
```

9. Definujte kanál CLUSSDR na správci front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from NEWYORK to repository at LONDON')
```

10. Definujte frontu klastru INVENTQ

Definujte frontu INVENTQ ve správci front NEWYORK zadáním klíčového slova CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)  
AMQ8006: Websphere MQ queue created.
```

Klíčové slovo CLUSTER způsobí, že fronta bude inzerována do klastru. Jakmile je fronta definována, bude zpřístupněna pro ostatní správce front v klastru. Mohou do ní odesílat zprávy, aniž by bylo nutné pro ni vytvořit definici vzdálené fronty.

Všechny definice jsou dokončené. Na všech platformách spusťte program modulu listener na každém správci front. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

Nastavení klastru pomocí LU 6.2 na systému z/OS

Postup

1. Rozhodněte se pro organizaci klastru a jeho název.

Rozhodli jste se propojit dva správce front, LONDON a NEWYORK, do klastru. Klaster s pouze dvěma správci front nabízí pouze okrajovou výhodu v rámci sítě, která má používat distribuované řazení do fronty. Je to dobrý způsob, jak začít, a poskytuje prostor pro budoucí expanzi. Když otevřete nové větve svého úložiště, můžete do klastru snadno přidávat nové správce front. Přidání nových správců front nenaruší existující síť; viz [“Přidání správce front do klastru”](#) na stránce 238.

Prozatím se jedná o jedinou aplikaci, kterou spouštíte, je aplikace inventarizace. Název klastru je INVENTORY.

2. Rozhodněte se, které správce front mají uchovávat úplná úložiště.

V každém klastru musíte navrhnout alespoň jednoho správce front, nebo nejlépe dva, aby se udržela úplná úložiště. V tomto příkladu jsou pouze dva správce front, LONDON a NEWYORK, z nichž obě zadržují úplná úložiště.

- a. Zbývající kroky můžete provést v libovolném pořadí.
- b. Při dalším postupu mohou být varovné zprávy zapsány do systémové konzoly produktu z/OS . Zprávy jsou výsledkem chybějících definic, které jste ještě přidali.
- c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštěni správce front.

3. Upravte definice správce front tak, aby byly přidány definice úložiště.

V každém správci front, který má uchovávat úplné úložiště, změňte definici lokální správce front pomocí příkazu ALTER QMGR a zadáním atributu REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)  
AMQ8005: Websphere MQ queue manager changed.
```

Zadáte-li například:

- a. runmqsc LONDON
- b. ALTER QMGR REPOS(INVENTORY)

LONDON se změní na úplné úložiště.

4. Definujte moduly listener.

Listener není spuštěn, když je definován, takže musí být ručně spuštěn poprvé s následujícím příkazem MQSC:

```
START LISTENER(LONDON_LS)
```

Vydejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každou z nich.

5. Definujte kanál CLUSRCVR pro správce front LONDON .

V každém správci front v klastru můžete definovat kanál příjemce klastru, v němž může správce front přijímat zprávy. Viz [Channel-receiver channel: CLUSRCVR](#) . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, na které se mohou odkazovat další správci front. Klíčové slovo CLUSTER zobrazuje dostupnost správce front pro příjem zpráv od jiných správců front v klastru.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager LONDON')
AMQ8014: Websphere MQ channel created.
07/09/98 12:56:35 No repositories for cluster 'INVENTORY'
```

6. Definujte kanál CLUSRCVR pro správce front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNNAME(NEWYORK.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager NEWYORK')
```

7. Definujte kanál CLUSSDR na správci front LONDON .

Kanál CLUSSDR můžete ručně definovat ze všech správců front úplného úložiště do všech ostatních správců front úplného úložiště v klastru. Viz [Odesílací kanál klastru: CLUSSDR](#) . V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který ukazuje na kanál CLUSRCVR definovaný v jiném správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Má-li správce front definice pro kanál příjemce klastru a odesílací kanál klastru ve stejném klastru, bude kanál odesílatele klastru spuštěn.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNNAME(CPIC) CLUSTER(INVENTORY)
DESCR('LU62 Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNNAME(NEWYORK.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: Websphere MQ channel created.
07/09/98 13:00:18 Channel program started.
```

8. Definujte kanál CLUSSDR na správci front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
```

```
CONNNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
DESCR('LU62 Cluster-sender channel from NEWYORK to repository at LONDON')
```

9. Definujte frontu klastru INVENTQ

Definujte frontu INVENTQ ve správci front NEWYORK zadáním klíčového slova CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: Websphere MQ queue created.
```

Klíčové slovo CLUSTER způsobí, že fronta bude inzerována do klastru. Jakmile je fronta definována, bude zpřístupněna pro ostatní správce front v klastru. Mohou do ní odesílat zprávy, aniž by bylo nutné pro ni vytvořit definici vzdálené fronty.

Všechny definice jsou dokončené. Na všech platformách spusťte program modulu listener na každém správci front. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

Ověření klastru

Informace o této úloze

Klastr můžete ověřit jedním nebo více z těchto způsobů:

1. Spuštění administrativních příkazů pro zobrazení atributů klastru a kanálu.
2. Spusťte ukázkové programy pro odesílání a příjem zpráv ve frontě klastru.
3. Napište své vlastní programy, které odešlou zprávu požadavku do fronty klastru a odpoví zprávou s odpovědí na neklastrovaná frontu odpovědí.

Postup

Chcete-li ověřit klastr, zadejte příkaz **DISPLAY runmqsc** .

Odpovědi, které vidíte, by měly být jako reakce v krocích, které následují.

1. Ve správci front NEWYORK spusťte příkaz **DISPLAY CLUSQMGR** :

```
dis clusqmgr(*)
```

```
1 : dis clusqmgr(*)
AMQ8441: Display Cluster Queue Manager details.
CLUSQMGR(NEWYORK) CLUSTER(INVENTORY)
CHANNEL(INVENTORY.NEWYORK)
AMQ8441: Display Cluster Queue Manager details.
CLUSQMGR(LONDON) CLUSTER(INVENTORY)
CHANNEL(INVENTORY.LONDON)
```

2. Ve správci front NEWYORK spusťte příkaz **DISPLAY CHANNEL STATUS** :

```
dis chstatus(*)
```

```

1 : dis chstatus(*)
AMQ8417: Display Channel Status details.
CHANNEL(INVENTORY.NEWYORK) XMITQ( )
CONNNAME(192.0.2.0) CURRENT
CHLTYPE(CLUSRCVR) STATUS(RUNNING)
RQMNAME(LONDON)
AMQ8417: Display Channel Status details.
CHANNEL(INVENTORY.LONDON) XMITQ(SYSTEM.CLUSTER.TRANSMIT.INVENTORY.LONDON)
CONNNAME(192.0.2.1) CURRENT
CHLTYPE(CLUSSDR) STATUS(RUNNING)
RQMNAME(LONDON)

```

Odesílání zpráv mezi dvěma správci front pomocí produktu **amqspu**t.

3. V systému LONDON spusťte příkaz **amqspu**t **INVENTQ LONDON**.

Zadejte některé zprávy, za nimiž bude následovat prázdný řádek.

4. V systému NEWYORK spusťte příkaz **amqsge**t **INVENTQ NEWYORK**.

Nyní uvidíte zprávy, které jste zadali v systému LONDON. Po 15 sekundách se program ukončí.

Odesílání zpráv mezi dvěma správci front pomocí vašich vlastních programů.

V následujících krocích vloží LONDON zprávu do INVENTQ na NEWYORK a obdrží odpověď ve své frontě LONDON_reply.

5. V systému LONDON vložte zprávy do fronty klastru.

- a) Definujte lokální frontu s názvem LONDON_reply.
- b) Nastavte volby MQOPEN na hodnotu MQOO_OUTPUT.
- c) Zadejte volání MQOPEN pro otevření fronty INVENTQ.
- d) Nastavte název *ReplyToQ* v deskriptoru zpráv na LONDON_reply.
- e) Zadejte volání příkazu MQPUT pro vložení zprávy.
- f) Potvrďte zprávu.

6. V systému NEWYORK obdrží zprávu ve frontě klastru a vložte odpověď do fronty odpovědí.

- a) Nastavte volby MQOPEN na hodnotu MQOO_BROWSE.
- b) Zadejte volání MQOPEN pro otevření fronty INVENTQ.
- c) Chcete-li získat zprávu z produktu INVENTQ, zadejte volání MQGET.
- d) Načtěte název *ReplyToQ* z deskriptoru zprávy.
- e) Zadejte název *ReplyToQ* do pole `ObjectName` deskriptoru objektu.
- f) Nastavte volby MQOPEN na hodnotu MQOO_OUTPUT.
- g) Zadejte volání MQOPEN pro otevření LONDON_reply ve správci front LONDON.
- h) Zadejte volání příkazu MQPUT pro vložení zprávy do produktu LONDON_reply.

7. V systému LONDON obdržíte odpověď.

- a) Nastavte volby MQOPEN na hodnotu MQOO_BROWSE.
- b) Zadejte volání MQOPEN pro otevření fronty LONDON_reply.
- c) Zadejte volání produktu MQGET , abyste získali zprávu z produktu LONDON_reply.

Přidání správce front do klastru

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí jedné přenosové fronty klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastř INVENTORY je nastaven tak, jak je popsáno v tématu “Nastavení nového klastřu” na stránce 228. Obsahuje dva správce front, produkty LONDON a NEWYORK, které uchovávají úplná úložiště.
- Správce front PARIS je vlastněn primární instalací. Pokud tomu tak není, musíte spustit příkaz **setmqenv**, který nastaví prostředí příkazu pro instalaci, do které patří produkt PARIS .
- Konektivita TCP existuje mezi všemi třemi systémy a správce front je konfigurován s modulem listener TCP, který začíná pod kontrolou správce front.

Informace o této úloze

1. Nová větev úložiště řetězce je nastavována v Paříži a vy chcete přidat správce front s názvem PARIS do klastřu.
2. Správce front PARIS odesílá aktualizace soupisu do aplikace běžící na systému v New Yorku vložením zpráv do fronty INVENTQ .

Chcete-li přidat správce front do klastřu, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště PARIS odkazuje na první.

Každý správce front v klastřu musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastřu z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile se nový správce front přidá do klastřu, ihned se naučí také o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu propojíte PARIS se správcem front LONDON, a to čistě z geografických důvodů.

Poznámka: Proveďte zbývající kroky v libovolném pořadí, po spuštění správce front PARIS .

2. Definujte kanál CLUSRCVR ve správci front PARIS.

Každý správce front v klastřu musí definovat kanál příjemce klastřu, ve kterém může přijímat zprávy. V systému PARIS definujte:

```
DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-receiver channel for queue manager PARIS')
```

Přijímací kanál klastřu oznamuje dostupnost zpráv od jiných správců front v klastřu INVENTORY. Nevytvářet definice v jiných správcích front pro odeslání do kanálu příjemce klastřu INVENTORY . PARIS. Další definice se automaticky provedou, když je třeba. Viz [Kanály klastřu](#).

3. 

Spusťte inicializátor kanálu na serveru IBM MQ for z/OS.

4. Definujte kanál CLUSSDR ve správci front PARIS.

Přidáte-li do klastřu správce front, který není úplným úložištěm, definujte pouze jeden kanál odesílatele klastřu, aby se počáteční připojení k úplnému úložišti stalo počátečními. Viz [Odesílací kanál klastřu: CLUSSDR](#) .

V systému PARIS vytvořte následující definici pro kanál CLCLSDR s názvem INVENTORY . LONDON ke správci front se síťovou adresou LONDON . CHSTORE . COM.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at LONDON')
```

5. Volitelné: Pokud přidáváte do klastřu správce front, který byl již dříve odebrán ze stejného klastřu, zkontrolujte, zda se nyní zobrazuje jako člen klastřu. Pokud ne, proveďte následující dodatečné kroky:
 - a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, který přidáváte.

Tento krok zastaví kanály klastru a poskytne lokální mezipaměti klastru čerstvou sadu pořadových čísel, která jsou zajištěná tak, aby byla ve zbývající části klastru až do konce.

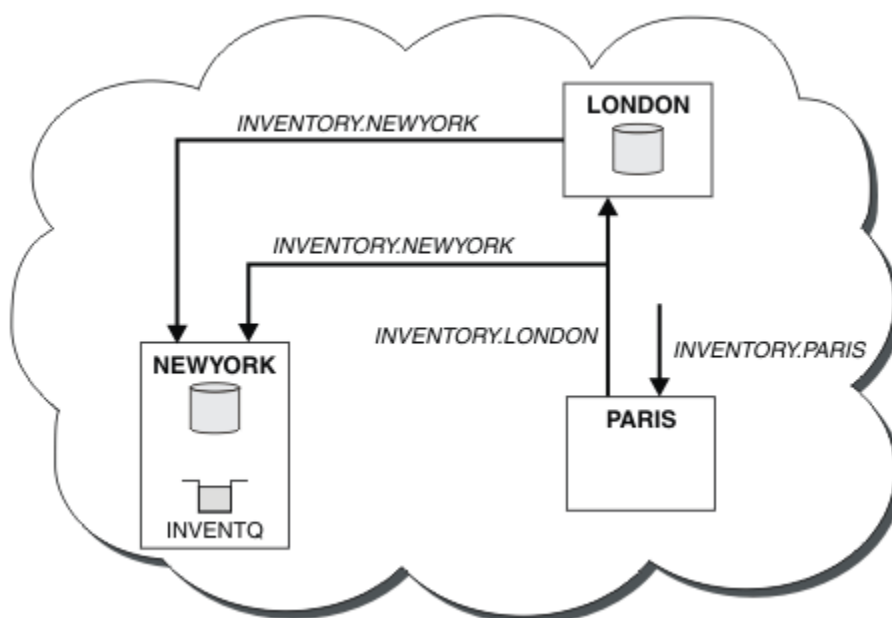
```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

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](#).

- b) Restartujte kanál CLUSSDR
(příklad pomocí příkazu `START CHANNEL`).
- c) Restartujte kanál CLUSRCVR.

Výsledky

Následující obrázek ukazuje klastr, který je nastaven touto úlohou.



Obrázek 40. Klastr INVENTORY se třemi správci front

Při vytváření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR jsme přidali správce front PARIS do klastru.

Nyní se správce front produktu PARIS učí z úplného úložiště na serveru LONDON, že fronta INVENTQ je hostována správcem front NEWYORK. Když se aplikace hostovaná v systému v Paříži pokusí vložit zprávy do INVENTQ, PARIS automaticky definuje odesílací kanál klastru pro připojení k přijímacímu kanálu klastru INVENTORY . NEWYORK. Aplikace může přijímat odpovědi, je-li zadán název správce front jako cílového správce front a že je poskytnuta fronta pro odpověď.

Přidání správce front do klastru: samostatné přenosové fronty

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Než začnete

- Správce front není členem žádného klastru.
- Klastr existuje; existuje úplné úložiště, ke kterému se tento správce front může připojit přímo a k dispozici úložiště. Postup vytvoření klastru viz [“Nastavení nového klastru”](#) na stránce 228.

Informace o této úloze

Tato úloha je alternativou k produktu “Přidání správce front do klastru” na stránce 238, ve kterém přidáváte správce front do klastru, který umísťuje zprávy klastru do jediné přenosové fronty.

V této úloze přidáte správce front do klastru, který automaticky vytvoří oddělené přenosové fronty klastru pro každý odesílací kanál klastru.

Chcete-li zachovat malý počet definic front, použijte se výchozí nastavení pro použití jediné přenosové fronty. Použití samostatných přenosových front je výhodné, chcete-li monitorovat provoz určený pro různé správce front a různé klastry. Chcete-li dosáhnout cíle izolace nebo výkonu, můžete také chtít oddělit provoz k různým místům určení.

Postup

1. Změňte výchozí typ přenosové fronty kanálu klastru.

Změňte správce front PARIS:

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

Pokaždé, když správce front vytvoří odesílací kanál klastru k odeslání zprávy správci front, vytvoří přenosovou frontu klastru. Přenosová fronta je používána pouze tímto odesílacím kanálem klastru. Přenosová fronta je trvalá-dynamická. Vytvoří se z modelové fronty SYSTEM . CLUSTER . TRANSMIT . MODEL . QUEUEs názvem SYSTEM . CLUSTER . TRANSMIT . *ChannelName*.



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**.

2. Rozhodněte se, které úplné úložiště PARIS odkazuje na první.

Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile se nový správce front přidá do klastru, ihned se naučí také o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu propojíte PARIS se správcem front LONDON, a to čistě z geografických důvodů.

Poznámka: Proved'te zbývající kroky v libovolném pořadí, po spuštění správce front PARIS .

3. Definujte kanál CLUSRCVR ve správci front PARIS.

Každý správce front v klastru musí definovat kanál příjemce klastru, ve kterém může přijímat zprávy. V systému PARISdefinujte:

```
DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)  
CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)  
DESCR('Cluster-receiver channel for queue manager PARIS')
```

Přijímací kanál klastru oznamuje dostupnost zpráv od jiných správců front v klastru INVENTORY. Nevytvářejte definice v jiných správcích front pro odeslání do kanálu příjemce klastru INVENTORY . PARIS. Další definice se automaticky provedou, když je třeba. Viz [Kanály klastru](#).

4. Definujte kanál CLUSSDR ve správci front PARIS.

Přidáte-li do klastru správce front, který není úplným úložištěm, definujte pouze jeden kanál odesílatele klastru, aby se počáteční připojení k úplnému úložišti stalo počátečními. Viz [Odesílací kanál klastru: CLUSSDR](#) .

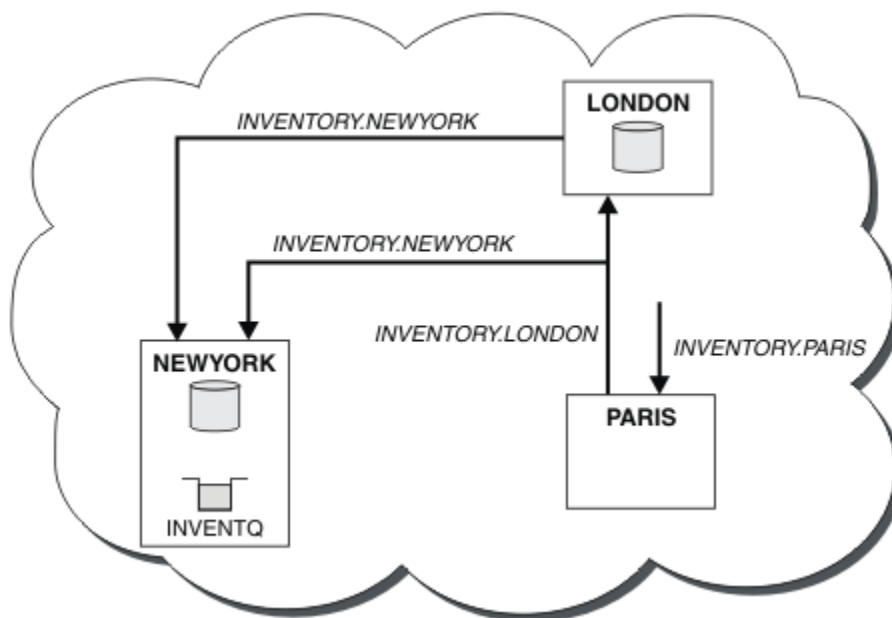
V systému PARIS vytvořte následující definici pro kanál CLCLSDR s názvem INVENTORY . LONDON ke správci front se síťovou adresou LONDON . CHSTORE . COM.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at LONDON')
```

Správce front automaticky vytvoří trvalou přenosovou frontu dynamického klastru SYSTEM . CLUSTER . TRANSMIT . INVENTORY . LONDON ze modelové fronty SYSTEM . CLUSTER . TRANSMIT . MODEL . QUEUE. Nastavuje atribut CLCHNAME přenosové fronty na INVENTORY . LONDON.

Výsledky

Následující obrázek ukazuje klastr, který je nastaven touto úlohou.



Obrázek 41. Klastr INVENTORY se třemi správci front

Při vytváření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR jsme přidali správce front PARIS do klastru.

Nyní se správce front produktu PARIS učí z úplného úložiště na serveru LONDON, že fronta INVENTQ je hostována správcem front NEWYORK. Když se aplikace hostovaná v systému v Paříži pokusí vložit zprávy do INVENTQ, PARIS automaticky definuje odesílací kanál klastru pro připojení k přijímacímu kanálu klastru INVENTORY . NEWYORK. Aplikace může přijímat odpovědi, je-li zadán název správce front jako cílového správce front a že je poskytnuta fronta pro odpověď.

Související úlohy

Přidání správce front do klastru pomocí protokolu DHCP

Přidejte správce front do klastru pomocí protokolu DHCP. Úloha demonstruje vynechání hodnoty CONNAME v definici CLUSRCVR .

Přidání správce front do klastru pomocí protokolu DHCP

Přidejte správce front do klastru pomocí protokolu DHCP. Úloha demonstruje vynechání hodnoty CONNAME v definici CLUSRCVR .

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Úloha demonstruje dvě speciální funkce:

- Možnost vynechat hodnotu parametru CONNAME v definici CLUSRCVR .
- Schopnost používat produkt +QMNAME+ v definici CLUSSDR .

Ani jedna z funkcí není poskytována v produktu z/OS.

Scénář:

- Klastř INVENTORY byl nastaven tak, jak je popsáno v tématu “Nastavení nového klastru” na stránce [228](#). Obsahuje dva správce front, produkty LONDON a NEWYORK, které uchovávají úplná úložiště.
- Nová větev úložiště řetězce je nastavována v Paříži a vy chcete přidat správce front s názvem PARIS do klastru.
- Správce front PARIS odesílá aktualizace soupisu do aplikace běžící na systému v New Yorku vložení zpráv do fronty INVENTQ.
- Síťová konektivita existuje mezi všemi třemi systémy.
- Síťový protokol je TCP.
- Systém správce front produktu PARIS používá protokol DHCP, což znamená, že adresy IP se mohou při restartování systému změnit.
- Kanály mezi systémy PARIS a LONDON jsou pojmenovány podle definované konvence pojmenování. Konvence používá název správce front úplného úložiště v produktu LONDONsprávce front.
- Administrátoři správce front produktu PARIS nemají k dispozici žádné informace o názvu správce front v úložišti LONDON . Název správce front v úložišti LONDON se může změnit.

Informace o této úloze

Chcete-li přidat správce front do klastru pomocí protokolu DHCP, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště PARIS odkazuje na první.

Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile se nový správce front přidá do klastru, ihned se naučí také o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu se rozhodneme propojit PARIS se správcem front LONDON, a to čistě z geografických důvodů.

Poznámka: Proveďte zbývající kroky v libovolném pořadí, po spuštění správce front PARIS .

2. Definujte kanál CLUSRCVR ve správci front PARIS.

Každý správce front v klastru musí definovat kanál příjemce klastru, na kterém může přijímat zprávy. V systému PARISdefinujte:

```
DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR)
TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('Cluster-receiver channel for queue manager PARIS')
```

Přijímací kanál klastru oznamuje dostupnost zpráv od jiných správců front v klastru INVENTORY. Není třeba uvádět parametr CONNAME na přijímacím kanálu klastru. Můžete požádat IBM MQ o zjištění jména připojení ze systému, buď vynecháním CONNAME, nebo zadáním CONNAME(' '). IBM MQ vygeneruje hodnotu CONNAME pomocí aktuální adresy IP systému; viz [CONNAME](#) . Není třeba vytvářet definice pro ostatní správce front pro odeslání na přijímací kanál klastru INVENTORY .PARIS. Další definice se automaticky provedou, když je třeba.

3. Definujte kanál CLUSSDR ve správci front PARIS.

Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na který může odesílat zprávy do svého počátečního úplného úložiště. V systému PARIS vytvořte následující definici pro kanál s názvem INVENTORY . +QMNAME+ ke správci front s adresou sítě LONDON . CHSTORE . COM.

```
DEFINE CHANNEL(INVENTORY.+QMNAME+) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at LONDON')
```

4. Volitelné: Pokud přidáváte do klastru správce front, který byl již dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:

a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, který přidáváte.

Tento krok zastaví kanály klastru a poskytne lokální mezipaměti klastru čerstvou sadu pořadových čísel, která jsou zajištěná tak, aby byla ve zbývajících částech klastru až do konce.

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

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](#).

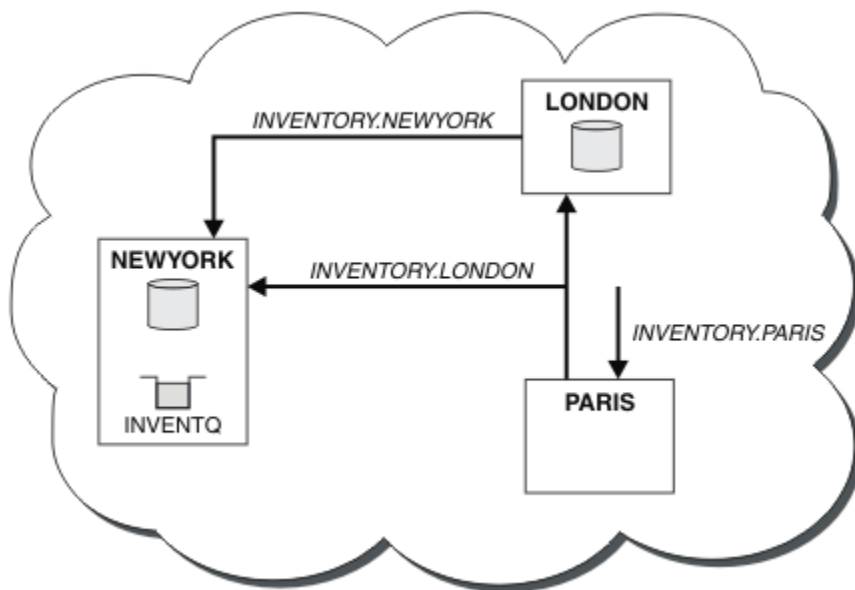
b) Restartujte kanál CLUSSDR

(příklad pomocí příkazu `START CHANNEL`).

c) Restartujte kanál CLUSRCVR.

Výsledky

Klastr nastavený touto úlohou je stejný jako u produktu [“Přidání správce front do klastru”](#) na stránce 238:



Obrázek 42. Klastr INVENTORY se třemi správci front

Při vytváření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR jsme přidali správce front PARIS do klastru.

Na správci front produktu PARIS se spustí CLUSSDR obsahující řetězec +QMNAME+ . V systému LONDON se IBM MQ interpretuje jako +QMNAME+ na název správce front (LONDON). IBM MQ se pak shoduje s definicí kanálu s názvem INVENTORY . LONDON na odpovídající definici CLUSRCVR .

Produkt IBM MQ odešle zpět vyřešený název kanálu do správce front produktu PARIS . V systému PARIS je definice kanálu CLCLSDR pro kanál s názvem INVENTORY . +QMNAME+ nahrazena interně generovanou definicí CLCLSDR pro INVENTORY . LONDON. Tato definice obsahuje vyřešený název kanálu, ale jinak je stejný jako definice +QMNAME+ , kterou jste vytvořili. Úložiště klastru jsou rovněž uvedena spolu s definicí kanálu s nově vyřešeným názvem kanálu.

Poznámka:

1. Kanál vytvořený s názvem +QMNAME+ bude okamžitě neaktivní. Nikdy se nepoužívá k přenosu dat.
2. Uživatelské procedury kanálu mohou zobrazit změnu názvu kanálu mezi jedním vyvoláním a dalším vyvoláním.

Nyní se správce front produktu PARIS učí z úložiště v systému LONDON, že je hostitelem fronty INVENTORY správce front NEWYORK. Když se aplikace hostovaná v systému v Paříži pokouší vložit zprávy do INVENTORY , PARIS automaticky, definuje odesílací kanál klastru pro připojení k přijímacímu kanálu klastru INVENTORY . NEWYORK. Aplikace může přijímat odpovědi, je-li zadán název správce front jako cílového správce front a že je poskytnuta fronta pro odpověď.

Související úlohy

Přidání správce front do klastru: samostatné přenosové fronty

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Související informace

Definovat kanál

Přidání správce front, který je hostitelem fronty

Přidejte do klastru jiného správce front, aby bylo hostitelem jiné fronty produktu INVENTORY . Požadavky se odesílají střídavě do front v každém správci front. V existujícím hostiteli produktu INVENTORY není třeba provést žádné změny.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klaster INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 238. Obsahuje tři správce front; LONDON a NEWYORK udržují úplná úložiště, PAŘÍŽ obsahuje dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK . Aplikace je řízena doručení zprávy ve frontě INVENTORY .
- V Torontu se vytváří nové prodejny. Chcete-li poskytnout další kapacitu, chcete-li spustit aplikaci soupisu na systému v Torontu stejně jako v New Yorku.
- Síťová konektivita existuje mezi všemi čtyřmi systémy.
- Síťový protokol je TCP.

Poznámka: Správce front TORONTO obsahuje pouze dílčí úložiště. Chcete-li do klastru přidat správce front úplného úložiště, přečtěte si téma “Přesunutí úplného úložiště do jiného správce front” na stránce 249.

Informace o této úloze

Chcete-li přidat správce front, který je hostitelem fronty, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště TORONTO odkazuje na první.

Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. To není zvláštní

význam, který úložiště si vyberete. V tomto příkladě si zvolíme NEWYORK. Poté, co se nový správce front připojil ke klastru, komunikuje s oběma úložišti.

2. Definujte kanál CLUSRCVR .

Každý správce front v klastru musí definovat kanál příjemce klastru, na kterém může přijímat zprávy. V systému TORONTO definujte kanál CLUSRCVR :

```
DEFINE CHANNEL(INVENTORY.TORONTO) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNNAME(TORONTO.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-receiver channel for TORONTO')
```

Správce front produktu TORONTO inzeruje svou dostupnost přijímat zprávy od jiných správců front v klastru INVENTORY pomocí kanálu příjemce klastru.

3. Definujte kanál CLUSSDR ve správci front TORONTO.

Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě vyberte volbu NEWYORK. Produkt TORONTO potřebuje následující definici:

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from TORONTO to repository at NEWYORK')
```

4. Volitelné: Pokud přidáváte do klastru správce front, který byl již dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:

a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, který přidáváte.

Tento krok zastaví kanály klastru a poskytne lokální mezipaměti klastru čerstvou sadu pořadových čísel, která jsou zajištěná tak, aby byla ve zbývajících částech klastru až do konce.

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

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](#).

b) Restartujte kanál CLUSSDR

(příklad pomocí příkazu [START CHANNEL](#)).

c) Restartujte kanál CLUSRCVR.

5. Přezkoumejte aplikaci soupisu pro afinity zpráv.

Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv a nainstaluje aplikaci na systém v Torontu.

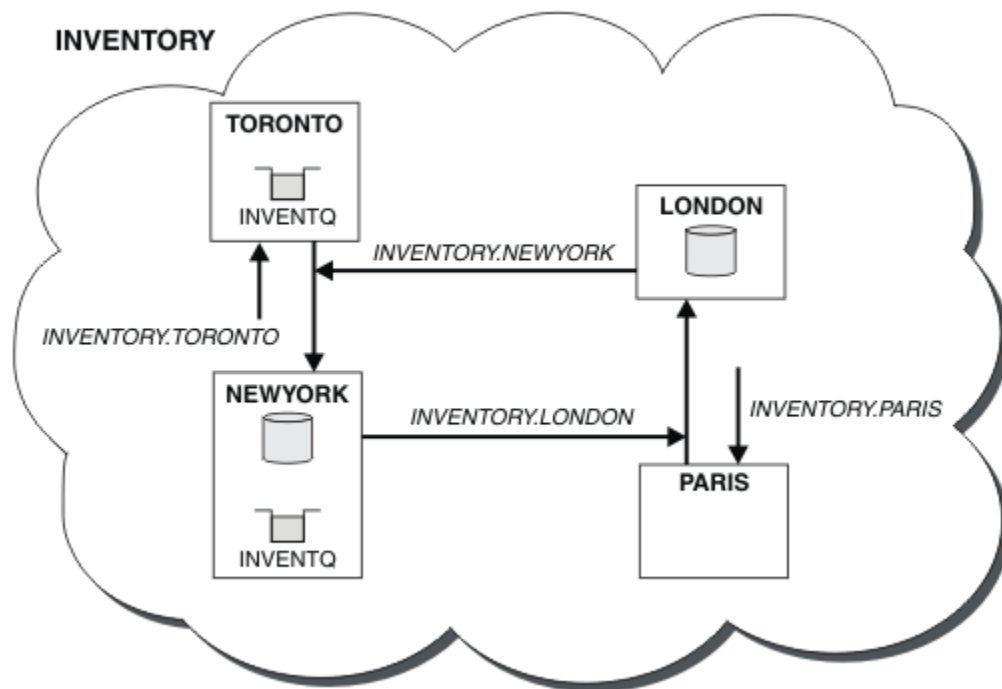
6. Definujte frontu klastru INVENTQ.

Frontu INVENTQ , která je již hostována správcem front NEWYORK , je také hostována pomocí TORONTO. Definujte jej ve správci front produktu TORONTO takto:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

Výsledky

[Obrázek 43 na stránce 247](#) zobrazuje klastr INVENTORY , který je nastaven touto úlohou.



Obrázek 43. Klastř INVENTORY se čtyřmi správci front

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správčích front v klastř. To zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje distribuci pracovní zátěže mezi dvěma správci front. Zprávy, které byly do produktu INVENTQ vloženy buď pomocí produktu TORONTO, nebo NEWYORK, jsou zpracovávány instancí v lokálním správci front, kdykoli je to možné. Zprávy ve verzi LONDON nebo PARIS jsou směřovány střídavě na TORONTO nebo NEWYORK, takže pracovní zátěž je vyvážená.

Tato úprava klastř byla dokončena, aniž byste museli měnit definice ve správčích front NEWYORK, LONDON a PARIS. Úplná úložiště v těchto správčích front jsou aktualizována automaticky s informacemi, které potřebují k odesílání zpráv do produktu INVENTQ na adrese TORONTO. Aplikace inventáře pokračuje ve funkci, pokud se jeden z NEWYORK nebo správce front TORONTO stane nedostupným a má dostatečnou kapacitu. Aplikace soupisu musí být schopna pracovat správně, je-li hostována na obou místech.

Jak můžete vidět z výsledku této úlohy, můžete mít stejnou aplikaci spuštěnou ve více než jednom správci front. Klastrování můžete rozdělit na pracovní zátěž rovnoměrně.

Aplikace nemusí být schopna zpracovat záznamy v obou lokalitách. Předpokládejme například, že jste se rozhodli přidat dotaz na zákaznický účet a aktualizovat aplikaci spuštěnou v produktu LONDON a NEWYORK. Záznam účtu může být zadržen pouze na jednom místě. Můžete se rozhodnout, že budete řídit distribuci požadavků pomocí techniky dělení dat na oblasti. Distribuci záznamů můžete rozdělit. Mohli byste uspořádat polovinu záznamů, například pro čísla účtů 00000-49999, které mají být zadrženy v LONDON. Druhá polovina, v rozsahu 50000-99999, se nachází v NEWYORK. Pak můžete napsat uživatelský program pracovní zátěže klastř a zkontrolovat pole účtu ve všech zprávách a směřovat zprávy do příslušného správce front.

Jak pokračovat dále

Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front TORONTO. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastř, je-li potřeba.

Přidání skupiny sdílení front do existujících klastrů

Přidejte skupinu sdílení front v systému z/OS do existujících klastrů.

Než začnete

Poznámka:

1. Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.
2. Skupiny sdílení front jsou podporovány pouze v systému IBM MQ for z/OS. Tato úloha se nevztahuje na jiné platformy.

Scénář:

- Klaster INVENTORY byl nastaven tak, jak je popsáno v tématu [“Nastavení nového klastru”](#) na stránce 228. Obsahuje dva správce front, LONDON a NEWYORK.
- Chcete přidat skupinu sdílení front do tohoto klastru. Skupina QSGPobsahuje tři správce front, P1, P2a P3. Sdílejí instanci fronty INVENTQ , která má být definována pomocí P1.

Informace o této úloze

Chcete-li přidat nové správce front, kteří jsou hostiteli sdílené fronty, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště budou správci front odkazovat jako první.

Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Není zvláštní význam toho, jaké úplné úložiště si vyberete. V tomto příkladu vyberte volbu NEWYORK. Jakmile se skupina sdílení front připojila ke klastru, komunikuje s oběma úplnými úložišti.

2. Definujte kanály CLUSRCVR .

Každý správce front v klastru musí definovat kanál příjemce klastru, na kterém může přijímat zprávy. V systémech P1, P2a P3definujte:

```
DEFINE CHANNEL(INVENTORY.Pn) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNNAME(Pn.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-receiver channel for sharing queue manager')
```

Přijímací kanál klastru oznamuje dostupnost jednotlivých správců front přijímat zprávy od jiných správců front v klastru INVENTORY.

3. Definujte kanál CLUSSDR pro skupinu sdílení front.

Každý člen klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK. Jeden ze správců front v rámci skupiny sdílení front potřebuje následující definici skupiny. Definice zajišťuje, že každý správce front má definici kanálu odesílatele klastru.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) QSGDISP(GROUP)
DESCR('Cluster-sender channel to repository at NEWYORK')
```

4. Definujte sdílenou frontu.

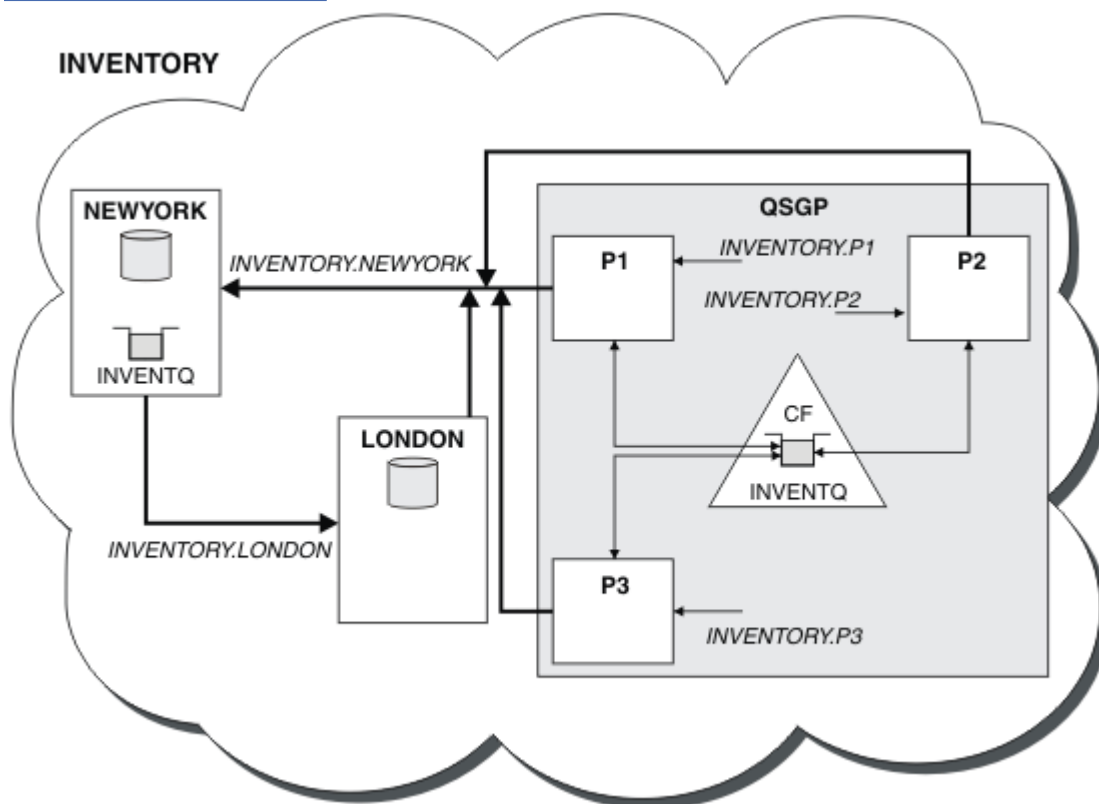
Definujte frontu INVENTQ v systému P1 tímto způsobem:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) QSGDISP(SHARED) CFSTRUCT(STRUCTURE)
```


Spusťte inicializátor kanálu a program modulu listener na novém správci front. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 44 na stránce 249 zobrazuje klastr nastavený touto úlohou.



Obrázek 44. Klastr a skupina sdílení front

Nyní jsou zprávy zařazené do fronty INVENTQ produktem LONDON směrovány střídavě po čtyřech správcích front, které jsou inzerovány jako hostování fronty.

Jak pokračovat dále

Výhoda, která má členy skupiny klastrů se sdílením front, je libovolný člen skupiny může odpovědět na požadavek. V takovém případě se produkt P1 stane nedostupným po přijetí zprávy ve sdílené frontě. Místo toho může odpovědět jiný člen skupiny sdílení front.

Přesunutí úplného úložiště do jiného správce front

Přemístění úplného úložiště z jednoho správce front do jiného a sestavení nového úložiště z informací uložených ve druhém úložišti.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu [“Přidání správce front do klastru”](#) na stránce 238.

- Z obchodních důvodů nyní chcete odebrat úplné úložiště ze správce front LONDONa nahradit jej úplným úložištěm ve správci front PARIS. Správce front produktu NEWYORK má pokračovat v držení úplného úložiště.

Informace o této úloze

Chcete-li přesunout úplné úložiště do jiného správce front, postupujte podle následujících kroků.

Postup

1. Upravte produkt PARIS tak, aby se z něj stalo správce front úplného úložiště.

V systému PARISzadejte následující příkaz:

```
ALTER QMGR REPOS(INVENTORY)
```

2. Přidejte kanál CLUSSDR na PARIS

PARIS má v současné době odesílací kanál klastru odkazující na LONDON. Produkt LONDON již nebude obsahovat úplné úložiště pro klastr. Produkt PARIS musí mít nový odesílací kanál klastru, který ukazuje na NEWYORK, kde je nyní zadrženo jiné úplné úložiště.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at NEWYORK')
```

3. Definujte kanál CLUSSDR na NEWYORK , který odkazuje na PARIS

V současné době má produkt NEWYORK kanál odesílatele klastru, který ukazuje na LONDON. Nyní, když se další úplné úložiště přesunulo do produktu PARIS, je třeba přidat nový odesílací kanál klastru v NEWYORK , který ukazuje na PARIS.

```
DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from NEWYORK to repository at PARIS')
```

Když přidáte kanál odesílatele klastru do produktu PARIS, produkt PARIS se dozví o klastru z produktu NEWYORK. Staví své vlastní úplné úložiště pomocí informací z produktu NEWYORK.

4. Zkontrolujte, zda má správce front PARIS nyní úplné úložiště.

Zkontrolujte, zda správce front PARIS vytvořil své vlastní úplné úložiště z úplného úložiště ve správci front NEWYORK. Zadejte následující příkazy:

```
DIS QCLUSTER(*) CLUSTER (INVENTORY)
DIS CLUSQMGR(*) CLUSTER (INVENTORY)
```

Zkontrolujte, zda tyto příkazy zobrazují podrobnosti o stejných prostředcích v tomto klastru jako v produktu NEWYORK.

Poznámka: Pokud správce front NEWYORK není k dispozici, nelze tuto budovu informací dokončit. Nepřesouvejte se na další krok, dokud nebude úloha dokončena.

5. Změnit definici správce front v systému LONDON

Nakonec změňte správce front na LONDON tak, aby již nezadržuje úplné úložiště pro klastr. V systému LONDONzadejte příkaz:

```
ALTER QMGR REPOS(' ')
```

Správce front již nebude přijímat žádné informace o klastrech. Po 30 dnech vyprší platnost informací uložených ve svém úplném úložišti. Správce front LONDON nyní hromadí své vlastní dílčí úložiště.

6. Odeberte nebo změňte všechny neprovedené definice.

Jste-li si jisti, že nové uspořádání klastru pracuje podle očekávání, odeberte nebo změňte ručně definované definice CLUSSDR, které již nejsou správné.

- Ve správci front PARIS je třeba zastavit a odstranit kanál odesílatele klastru do produktu LONDONa poté zadat příkaz ke spuštění kanálu, aby klastr mohl znovu použít automatické kanály:

```
STOP CHANNEL (INVENTORY.LONDON)
DELETE CHANNEL (INVENTORY.LONDON)
START CHANNEL (INVENTORY.LONDON)
```

- Ve správci front NEWYORK je třeba zastavit a odstranit kanál odesílatele klastru do produktu LONDONa poté zadat příkaz ke spuštění kanálu, aby klastr mohl znovu použít automatické kanály:

```
STOP CHANNEL (INVENTORY.LONDON)
DELETE CHANNEL (INVENTORY.LONDON)
START CHANNEL (INVENTORY.LONDON)
```

- Nahradte všechny ostatní ručně definované odesílací kanály klastru, které ukazují na LONDON ve všech správci front v klastru, s kanály, které ukazují na NEWYORK nebo PARIS. Po odstranění kanálu vždy zadejte příkaz **start channel**, aby klastr mohl opět používat automatické kanály. V tomto malém příkladu zde nejsou žádné další. Chcete-li zkontrolovat, zda jste zapomněli, zadejte příkaz `DISPLAY CHANNEL (*) TYPE (CLUSSDR)`. Příklad:

```
DISPLAY CHANNEL (*) TYPE (CLUSSDR)
```

Je důležité, abyste tuto úlohu provedli co nejdříve po přesunu úplného úložiště z produktu LONDON do produktu PARIS. Dříve než provedete tuto úlohu, správci front, kteří mají ručně definované kanály CLUSSDR s názvem INVENTORY.LONDON, mohou odesílat požadavky na informace prostřednictvím tohoto kanálu.

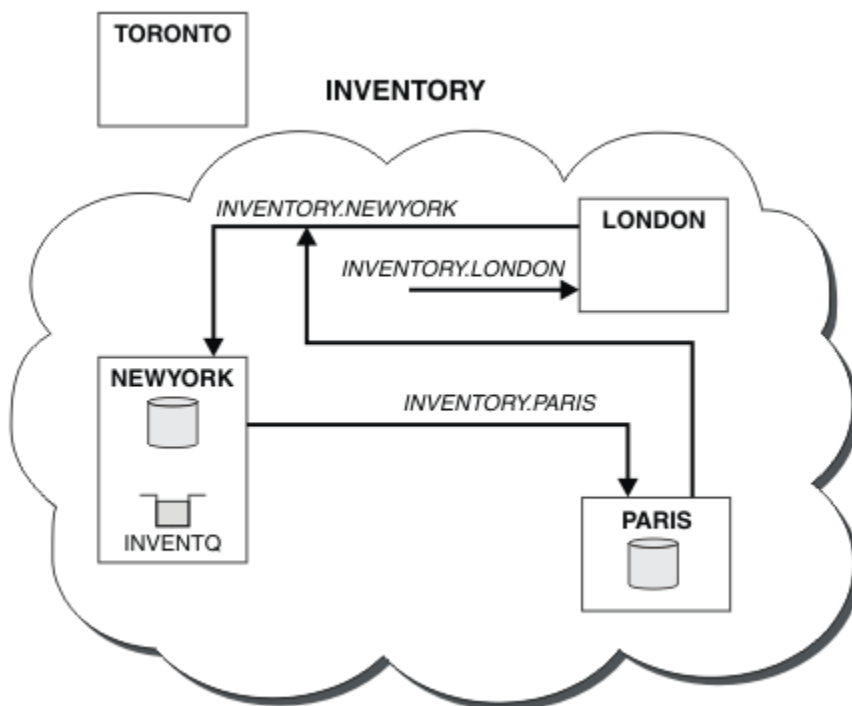
Poté, co produkt LONDON přestane být úplným úložištěm, pokud přijme takové požadavky, bude zapisovat chybové zprávy do svého protokolu chyb správce front. Následující příklady ukazují, které chybové zprávy se mohou zobrazit v produktu LONDON:

- AMQ9428: Unexpected publication of a cluster queue object received
- AMQ9432: Query received by a non-repository queue manager

Správce front LONDON neodpovídá na požadavky na informace, protože již není úplným úložištěm. Správci front, kteří požadují informace z produktu LONDON, se musí spoléhat na to, že informace o klastru budou záviset na NEWYORK, dokud nebudou ručně definované definice CLUSSDR opraveny tak, aby ukazovala na PARIS. Tato situace nesmí být tolerována jako platná konfigurace v dlouhodobém horizontu.

Výsledky

[Obrázek 45 na stránce 252](#) zobrazuje klastr nastavený touto úlohou.



Obrázek 45. Klastř INVENTORY s úplným úložištěm byl přesunut do PARIS

Ustanovení komunikace v klastru

Inicializátor kanálu je potřebný ke spuštění komunikačního kanálu, je-li k dispozici zpráva k doručení. Modul listener kanálu čeká na spuštění druhého konce kanálu, který má přijmout zprávu.

Než začnete

Chcete-li navázat komunikaci mezi správci front v klastru, nakonfigurujte propojení pomocí jednoho z podporovaných komunikačních protokolů. Podporované protokoly jsou TCP nebo LU 6.2 na libovolné platformě a NetBIOS nebo SPX na systémech Windows. Jako součást této konfigurace budete potřebovat také iniciátory kanálu a listenery kanálů stejně jako u distribuovaných front.

Informace o této úloze

Všichni správci front klastru potřebují inicializátor kanálu, aby monitoroval systémem definovanou inicializační frontu SYSTEM.CHANNEL.INITQ. SYSTEM.CHANNEL.INITQ je inicializační fronta pro všechny přenosové fronty včetně přenosové fronty klastru.

Každý správce front musí mít modul listener kanálu. Program modulu listener kanálu čeká na příchozí požadavky sítě a spustí příslušný přijímací kanál, je-li to potřeba. Implementace modulů listener kanálu je specifická pro platformu, nicméně existují některé běžné funkce. Na všech platformách IBM MQ lze modul listener spustit pomocí příkazu `START LISTENER`. V systémech IBM MQ for IBM i, Windows, SYSTÉM UNIX a Linux můžete modul listener spustit automaticky ve stejnou dobu jako správce front. Chcete-li modul listener spustit automaticky, nastavte atribut CONTROL na objekt LISTENER na hodnotu QMGR nebo STARTONLY.

z/OS Nesdílený port modulu listener (INDISP(QMGR)) musí být použit pro kanály CLUSRCVR na systému z/OS a pro kanály CLUSSDR na z/OS.

Postup

1. Spusťte inicializátor kanálu.

- ▶ **z/OS**

IBM MQ for z/OS

Pro každého správce front existuje jeden iniciátor kanálu a je spuštěn jako samostatný adresní prostor. Spustíte jej pomocí příkazu **MQSC START CHINIT** , který vydáváte jako součást spuštění správce front.

- ▶ **Windows** ▶ **Linux** ▶ **UNIX**

IBM MQ for Windows, systémy SYSTÉM UNIX a Linux

Když spustíte správce front, je-li atribut správce front SCHINIT nastaven na hodnotu QMGR, bude inicializátor kanálu automaticky spuštěn. Jinak může být spuštěn pomocí příkazu **runmqsc START CHINIT** nebo řídicího příkazu **runmqchi** .

- ▶ **IBM i**

IBM MQ for IBM i

Když spustíte správce front, je-li atribut správce front SCHINIT nastaven na hodnotu QMGR, bude inicializátor kanálu automaticky spuštěn. Jinak může být spuštěn pomocí příkazu **runmqsc START CHINIT** nebo řídicího příkazu **runmqchi** .

2. Spustíte modul listener kanálu.

- ▶ **z/OS**

IBM MQ for z/OS

Použijte program modulu listener kanálu poskytovaný produktem IBM MQ. Chcete-li spustit modul listener kanálu produktu IBM MQ , použijte příkaz **MQSC START LISTENER**, který je vydáváte jako součást spuštění inicializátoru kanálu. Příklad:

```
START LISTENER PORT(1414) TRPTYPE(TCP)
```

nebo:

```
START LISTENER LUNAME(LONDON.LUNAME) TRPTYPE(LU62)
```

Členové skupiny sdílení front mohou místo modulu listener pro každého správce front používat sdílený modul listener. Nepoužívejte sdílené moduly listener s klastry. Specificky nevytvářejte CONNAME objektu CLUSRCVR adresu sdíleného modulu listener skupiny sdílení front. Pokud tak učiníte, mohou správci front přijímat zprávy pro fronty, pro které nemají definici.

- ▶ **IBM i**

IBM MQ for IBM i

Použijte program modulu listener kanálu poskytovaný produktem IBM MQ. Chcete-li spustit modul listener kanálu produktu IBM MQ , použijte příkaz **CL STRMQLSR**. Příklad:

```
STRMQLSR MQMNAME(QM1) PORT(1414)
```

- ▶ **Windows**

IBM MQ for Windows

Použijte buď program modulu listener kanálu poskytovaný produktem IBM MQ, nebo prostředky poskytované operačním systémem.

Chcete-li spustit modul listener kanálu produktu IBM MQ , použijte příkaz **RUNMQLSR** . Příklad:

```
RUNMQLSR -t tcp -p 1414 -m QM1
```

- ▶ **Linux** ▶ **UNIX**

IBM MQ v systémech SYSTÉM UNIX a Linux

Použijte buď program modulu listener kanálu poskytovaný produktem IBM MQ, nebo prostředky poskytované operačním systémem; například **inetd** pro komunikaci TCP.

Chcete-li spustit modul listener kanálu produktu IBM MQ, použijte příkaz **runmqclsr**. Příklad:

```
runmqclsr -t tcp -p 1414 -m QM1
```

Chcete-li použít produkt **inetd** ke spuštění kanálů, nakonfigurujte dva soubory:

- Upravte soubor `/etc/services`. Musíte být přihlášení jako uživatel root nebo uživatel root. Pokud následující řádek není v souboru, přidejte jej podle obrázku:

```
MQSeries      1414/tcp      # Websphere MQ channel listener
```

kde 1414 je číslo portu vyžadované produktem IBM MQ. Můžete změnit číslo portu, ale musí se shodovat s číslem portu uvedeným na konci odesílání.

- Upravte soubor `/etc/inetd.conf`. Pokud v tomto souboru nemáte následující řádek, přidejte jej podle obrázku:

```
MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta  
-m queue.manager.name
```

kde `MQ_INSTALLATION_PATH` je nahrazen vysokoúrovňovým adresářem, ve kterém je nainstalován produkt IBM MQ.

Aktualizace se stanou aktivní poté, co produkt **inetd** znovu načte konfigurační soubory. Zadejte následující příkazy z ID uživatele root:

zapAIX:

```
refresh -s inetd
```

zapHP-UX:

```
inetd -c
```

V systémech Solaris nebo Linux:

- Vyhledejte ID procesu **inetd** pomocí příkazu:

```
ps -ef | grep inetd
```

- Spusťte příslušný příkaz následujícím způsobem:

- Pro Solaris 9 a Linux:

```
kill -1 inetd processid
```

- Pro verzi produktu Solaris 10 nebo novější:

```
inetconv
```

Převod existující sítě na klastr

Převeďte existující distribuovanou síť front do klastru a přidejte dalšího správce front za účelem zvýšení kapacity.

Než začnete

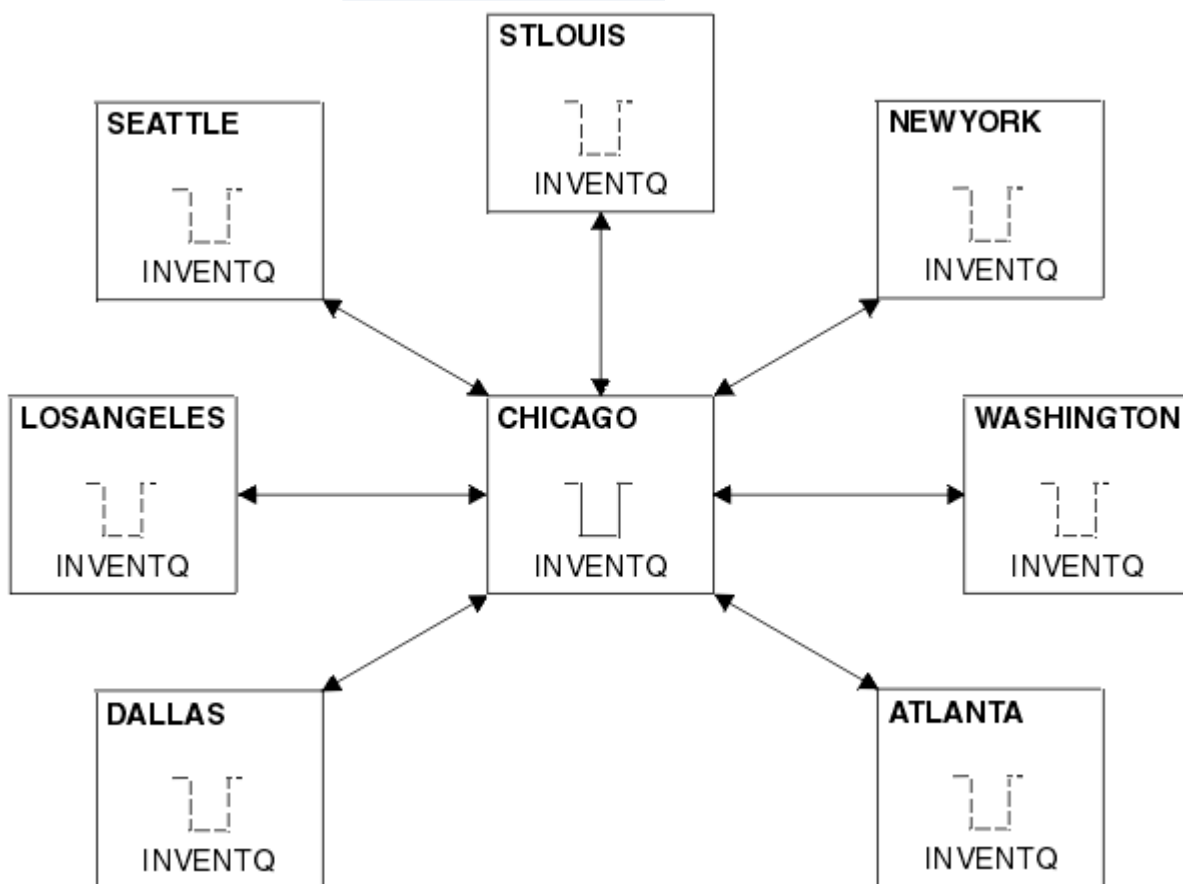
V produktu “Nastavení nového klastru” na stránce 228 až “Přesunutí úplného úložiště do jiného správce front” na stránce 249 jste vytvořili a rozšířili nový klastr. Následující dva úlohy zkoumají odlišný přístup: převod existující sítě správců front na klastr.

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Síť IBM MQ je již na místě, spojující celonárodní větve řetězové databáze. Má rozbočovač a paprsek paprsek: všichni správci front jsou připojeni k jednomu správci front. Správce centrální fronty se nachází v systému, na kterém je spuštěna aplikace zásob. Aplikace je řízena doručení zpráv ve frontě INVENTQ, pro které má každý správce front definici vzdálené fronty.

Tato síť je ilustrována v části [Obrázek 46](#) na stránce 255.



Obrázek 46. Centrální a paprsek paprsek

- Chcete-li usnadnit administraci, převedete tuto síť na klastr a vytvoříte v centrálním serveru jiného správce front, který bude sdílet pracovní zátěž.

Název klastru je CHNSTORE.

Poznámka: Název klastru CHNSTORE byl vybrán tak, aby názvy kanálů příjemce klastru, které mají být vytvořeny, byly vytvořeny s použitím názvů ve formátu *cluster-name.queue-manager*, které nepřesahují maximální délku 20 znaků, například CHNSTORE.WASHINGTON.

- Oba správci front jsou hostiteli úplných úložišť a jsou přístupné pro aplikaci soupisu.
- Aplikace inventáře se má řídit přijetím zpráv ve frontě produktu INVENTQ, jejímž hostitelem je některý z ústředních správců front.
- Aplikace v inventáři je jedinou aplikací spuštěnou paralelně a přístupnou více než jedním správcem front. Všechny ostatní aplikace budou nadále pracovat jako dříve.

- Všechny větve mají síťovou konektivitu ke dvěma centrálním správcům front.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li převést existující síť na klastr, postupujte podle následujících kroků.

Postup

1. Přezkoumejte aplikaci soupisu pro afinity zpráv.

Než budete pokračovat, ujistěte se, že aplikace dokáže zpracovat afinity zpráv. Afinity zpráv jsou vztahy mezi dialogovými zprávami, které se vyměňují mezi dvěma aplikacemi, kde zprávy musí být zpracovány určitým správcem front nebo v určité posloupnosti. Další informace o afinitě zprávy viz: [“Práce s afinitními zprávami”](#) na stránce 327

2. Upravte dva správce centrálních front, aby z nich učinili úplné správce front úložiště.

Dva správci front CHICAGO a CHICAG02 jsou na centrálním serveru této sítě. Rozhodli jste se soustředit veškerou aktivitu spojenou s klastrem úložiště řetězců na tyto dva správce front. Stejně jako aplikace inventarizace a definice pro frontu INVENTQ chcete těmto správcům front hostit dvě úplná úložiště v rámci klastru. V každém ze dvou správců front zadejte následující příkaz:

```
ALTER QMGR REPOS(CHNSTORE)
```

3. Definujte kanál CLUSRCVR pro každého správce front.

V každém správci front v klastru definujte kanál příjemce klastru a odesílací kanál klastru. Nezáleží na tom, který kanál definujete jako první.

Učinit definici CLUSRCVR za účelem inzerování každého správce front, jeho síťové adresy a dalších informací do klastru. Ve správci front ATLANTA například:

```
DEFINE CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNNAME(ATLANTA.CHSTORE.COM) CLUSTER(CHNSTORE)
DESCR('Cluster-receiver channel')
```

4. Definujte kanál CLUSSDR pro každého správce front.

Vytvořte v každém správci front definici CLUSSDR a propojte tohoto správce front s jedním nebo více správci front úplného úložiště. Můžete například propojit ATLANTA s CHICAG02:

```
DEFINE CHANNEL(CHNSTORE.CHICAG02) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(CHICAG02.CHSTORE.COM) CLUSTER(CHNSTORE)
DESCR('Cluster-sender channel to repository queue manager')
```

5. Nainstalujte aplikaci soupisu na CHICAG02.

You already have the inventory application on queue manager CHICAGO. Nyní je třeba vytvořit kopii této aplikace ve správci front CHICAG02.

6. Definujte frontu INVENTQ v centrálních správcích front.

V systému CHICAGO upravte definici lokální fronty pro frontu INVENTQ tak, aby byla fronta zpřístupněna pro klastr. Spusťte následující příkaz:

```
ALTER QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
```

V systému CHICAG02 vytvořte definici pro stejnou frontu:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
```


V systému z/OS můžete použít volbu MAKEDEF funkce COMMAND produktu **CSQUTIL** k vytvoření přesné kopie produktu CHICAGO2 v produktu INVENTQ v systému CHICAGO.

Když tyto definice provedete, odešle se zpráva do úplných úložišť na CHICAGO a CHICAGO2 a informace v nich se aktualizují. Správce front při vložení zprávy do produktu INVENTQ zjistí z úplných úložišť, že pro zprávy je k dispozici volba místa určení.

7. Zkontrolujte, že změny klastru byly rozšířeny.

Zkontrolujte, zda byly definice, které jste vytvořili v předchozím kroku, propagovány prostřednictvím klastru. Zadejte následující příkaz ve správci front úplného úložiště:

```
DIS QCLUSTER(INVENTQ)
```

Přidání nového propojeného klastru

Přidejte nový klaster, který bude sdílet některé správce front s existujícím klastrem.

Než začnete

Poznámka:

1. Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.
2. Před spuštěním této úlohy zkontrolujte kolize názvů front a porozumíte důsledkům. Možná budete muset přejmenovat frontu nebo nastavit alias fronty před tím, než budete moci pokračovat.

Scénář:

- Klaster IBM MQ byl nastaven tak, jak je popsáno v tématu [“Převod existující sítě na klaster”](#) na stránce 254.
- Je třeba implementovat nový klaster s názvem MAILORDER . Tento klaster se skládá ze čtyř správců front, kteří jsou v klastru CHNSTORE , CHICAGO, CHICAGO2, SEATTLE a ATLANTA, a dva další správce front; HARTFORD a OMAHA. Aplikace MAILORDER běží na systému v Omaha, který je připojen ke správci front OMAHA. Je řízen ostatními správci front v klastru, který vkládá zprávy do fronty produktu MORDERQ .
- Úplná úložiště pro klaster produktu MAILORDER se udržují na dvou správcích front CHICAGO a CHICAGO2.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li přidat nový propojený klaster, postupujte podle následujících kroků.

Postup

1. Vytvořte seznam názvů klastrů názvů.

Správci front úplného úložiště na serveru CHICAGO a CHICAGO2 se nyní budou držet úplných úložišť pro oba klastery CHNSTORE a MAILORDER. Nejprve vytvořte seznam názvů obsahující názvy klastrů. Definujte seznam názvů v systémech CHICAGO a CHICAGO2 následujícím způsobem:

```
DEFINE NAMELIST(CHAINMAIL)
DESCR('List of cluster names')
NAMES(CHNSTORE, MAILORDER)
```

2. Upravte dvě definice správce front.

Nyní změňte dvě definice správce front na CHICAGO a CHICAGO2. V současné době tyto definice ukazují, že správci front uchovávají úplná úložiště pro klaster CHNSTORE. Změňte tuto definici tak, aby

ukazovaly, že správci front uchovávají úplná úložiště pro všechny klastry uvedené v seznamu názvů produktu CHAINMAIL . Změňte definice správce front CHICAGO a CHICAGO2 :

```
ALTER QMGR REPOS(' ') REPOSNL(CHAINMAIL)
```

3. Upravte kanály CLUSRCVR na systémech CHICAGO a CHICAGO2.

Definice kanálu CLUSRCVR v produktu CHICAGO a v produktu CHICAGO2 ukazují, že kanály jsou dostupné v klastru CHNSTORE. Je třeba změnit definici příjemce klastru tak, aby ukazujete, že jsou kanály dostupné pro všechny klastry uvedené v seznamu názvů CHAINMAIL . Změňte definici přijímacího zásobníku na CHICAGO:

```
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSRCVR)  
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

V CHICAGO2zadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSRCVR)  
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

4. Pozměňte kanály CLUSSDR na CHICAGO a CHICAGO2.

Změňte dvě definice kanálu CLUSSDR a přidejte seznam názvů. V CHICAGOzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)  
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

V CHICAGO2zadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)  
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

5. Vytvořte seznam názvů v systémech SEATTLE a ATLANTA.

Vzhledem k tomu, že SEATTLE a ATLANTA budou členy více než jednoho klastru, musíte vytvořit seznam názvů obsahující názvy klastrů. Definujte seznam názvů v systémech SEATTLE a ATLANTA následujícím způsobem:

```
DEFINE NAMELIST(CHAINMAIL)  
DESCR('List of cluster names')  
NAMES(CHNSTORE, MAILORDER)
```

6. Upravte kanály CLUSRCVR na systémech SEATTLE a ATLANTA.

Definice kanálu CLUSRCVR v produktu SEATTLE a v produktu ATLANTA ukazují, že kanály jsou dostupné v klastru CHNSTORE. Změňte definice přijímacích kanálů klastru tak, aby ukazujete, že jsou kanály dostupné pro všechny klastry uvedené v seznamu názvů CHAINMAIL . V SEATTLEzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.SEATTLE) CHLTYPE(CLUSRCVR)  
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

V ATLANTAzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR)  
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

7. Pozměňte kanály CLUSSDR na SEATTLE a ATLANTA.

Změňte dvě definice kanálu CLUSSDR a přidejte seznam názvů. V SEATTLEzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

V ATLANTAzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

8. Definujte kanály CLUSRCVR a CLUSSDR v systémech HARTFORD a OMAHA.

Ve dvou nových správcích front HARTFORD a OMAHAdefinujte příjemce klastru a odesílací kanály klastru. Nezáleží na tom, v jakém pořadí vytvoříte definice. V HARTFORDzadejte:

```
DEFINE CHANNEL(MAILORDER.HARTFORD) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(HARTFORD.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-receiver channel for HARTFORD')

DEFINE CHANNEL(MAILORDER.CHICAGO) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(CHICAGO.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-sender channel from HARTFORD to repository at CHICAGO')
```

V OMAHAzadejte:

```
DEFINE CHANNEL(MAILORDER.OMAHA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(OMAHA.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-receiver channel for OMAHA')

DEFINE CHANNEL(MAILORDER.CHICAGO) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(CHICAGO.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-sender channel from OMAHA to repository at CHICAGO')
```

9. Definujte frontu MORDERQ na OMAHA.

Konečným krokem pro dokončení této úlohy je definovat frontu MORDERQ ve správci front OMAHA. V OMAHAzadejte:

```
DEFINE QLOCAL(MORDERQ) CLUSTER(MAILORDER)
```

10. Zkontrolujte, že změny klastru byly rozšířeny.

Ujistěte se, že definice, které jste vytvořili s předchozími kroky, byly rozšířeny, ačkoli klastr. Vydejte následující příkazy ve správci front úplného úložiště:

```
DIS QCLUSTER (MORDERQ)
DIS CLUSQMGR
```

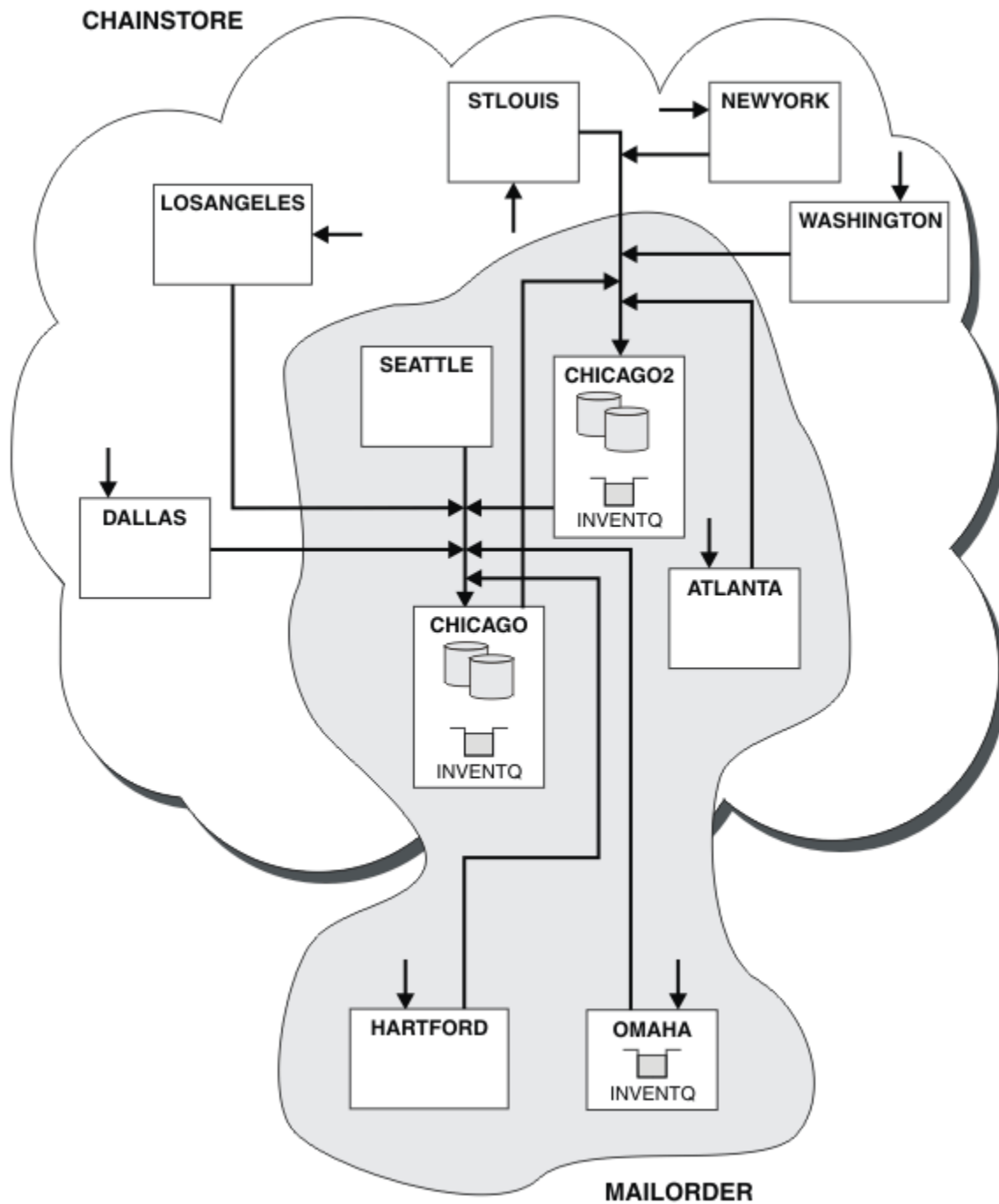
11.

Výsledky

Klastr nastavený touto úlohou se zobrazí v produktu [Obrázek 47](#) na stránce 260.

Nyní máme dva překrývající se klastry. Úplná úložiště pro oba klastry jsou drženy v CHICAGO a CHICAGO2. Aplikace pro objednávku pošty spuštěná v produktu OMAHA je nezávislá na aplikaci soupisu, která se spouští v produktu CHICAGO. Avšak někteří správci front, kteří jsou v klastru CHNSTORE , jsou také v klastru MAILORDER , a tak mohou odesílat zprávy do jedné z aplikací. Před provedením této úlohy se překrývají dva klastry a uvědomte si, že název fronty je v rozporu.

Předpokládejme, že v systémech NEWYORK v klastru CHNSTORE a v klastru OMAHA v klastru MAILORDERexistuje fronta s názvem ACCOUNTQ. Pokud překryvy klastry a poté aplikace v produktu SEATTLE vloží zprávu do fronty ACCOUNTQ, může tato zpráva přejít buď na instanci serveru ACCOUNTQ.



Obrázek 47. Propojené klastry

Jak pokračovat dále

Předpokládejme, že se rozhodnete sloučit klastr MAILORDER s klastrem CHNSTORE a vytvořit tak jeden velký klastr s názvem CHNSTORE.

Chcete-li sloučit klastr MAILORDER s klastrem CHNSTORE tak, aby CHICAGO a CHICAGO2 zadržovaly úplná úložiště, postupujte takto:

- Upravte definice správce front pro CHICAGO a CHICAGO2, odeberte atribut REPOSITE, který uvádí seznam názvů (CHAINMAIL), a nahradte jej atributem REPOS, který uvádí název klastru (CHNSTORE).
Například:

```
ALTER QMGR(CHICAGO) REPOSNL(' ') REPOS(CHNSTORE)
```

- U každého správce front v klastru MAILORDER změňte všechny definice kanálů a definice front tak, aby změnil hodnotu atributu CLUSTER z produktu MAILORDER na hodnotu CHNSTORE. Například v HARTFORDzadejte:

```
ALTER CHANNEL(MAILORDER.HARTFORD) CLUSTER(CHNSTORE)
```

V OMAHA zadejte:

```
ALTER QLOCAL(MORDERQ) CLUSTER(CHNSTORE)
```

- Upravte všechny definice, které uvádějí seznam názvů klastru CHAINMAIL, tj. definice kanálu CLUSRCVR a CLUSSDR na CHICAGO, CHICAGO2, SEATTLEa ATLANTA, aby bylo možné zadat místo toho klastr CHNSTORE.

V tomto příkladu můžete vidět tu výhodu použití seznamů názvů. Místo změny definic správce front pro CHICAGO a CHICAGO2 můžete změnit hodnotu seznamu názvů CHAINMAIL. Podobně, namísto změny definic kanálů CLUSRCVR a CLUSSDR na CHICAGO, CHICAGO2, SEATTLEa ATLANTAmůžete dosáhnout požadovaného výsledku změnou seznamu názvů.

Související úlohy

Odstranění sítě klastru

Odebrat klastr ze sítě a obnovit konfiguraci distribuované fronty.

Odstranění sítě klastru

Odebrat klastr ze sítě a obnovit konfiguraci distribuované fronty.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr IBM MQ byl nastaven tak, jak je popsáno v tématu [“Převod existující sítě na klastr”](#) na stránce 254.
- Tento klastr bude nyní odebrán ze systému. Síť správců front bude nadále fungovat stejně jako předtím, než byl klastr implementován.

Informace o této úloze

Chcete-li odebrat síť klastrů, postupujte takto.

Postup

1. Odeberte fronty klastru z klastru CHNSTORE .

V systémech CHICAGO a CHICAGO2upravte definici lokální fronty pro frontu INVENTQ tak, aby byla fronta odebrána z klastru. Spustte následující příkaz:

```
ALTER QLOCAL(INVENTQ) CLUSTER(' ')
```

Když změníte frontu, informace v úplných úložištích se aktualizují a šíří po celém klastru. Aktivní aplikace používající produkt MQ00_BIND_NOT_FIXEDa aplikace používající MQ00_BIND_AS_Q_DEF ,

kde byla fronta definována s DEFBIND (NOTFIXED), selžou při dalším pokusu o volání MQPUT nebo MQPUT1. Je vrácen kód příčiny MQRC_UNKNOWN_OBJECT_NAME.

Nejprve nemusíte provést krok 1, ale pokud jej neuděláte, proveďte ji namísto po kroku 4.

2. Zastavte všechny aplikace, které mají přístup k frontě klastru.

Zastavte všechny aplikace, které mají přístup k frontám klastru. Pokud neuděláte, mohou některé informace o klastru zůstat v lokálním správci front při aktualizaci klastru v kroku 5. Tyto informace se odeberou, když se zastaví všechny aplikace a kanály klastru se odpojí.

3. Odeberte atribut úložiště ze správců front úplného úložiště.

V produktu CHICAGO i v produktu CHICAGO2 upravte definice správce front tak, aby bylo možné odebrat atribut úložiště. Chcete-li to provést, zadejte příkaz:

```
ALTER QMGR REPOS(' ')
```

Správci front informují ostatní správce front v klastru o tom, že již nemají úplná úložiště. Pokud tyto informace obdrží ostatní správci front, zobrazí se zpráva označující, že bylo dokončeno úplné úložiště. Zobrazí se také jedna nebo více zpráv, které indikují, že již nejsou k dispozici žádná úložiště pro klastr CHNSTORE.

4. Odebrat kanály klastru.

V produktu CHICAGO odeberte kanály klastru:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR) CLUSTER(' ')
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSRCVR) CLUSTER(' ')
```

Poznámka: Je důležité nejprve zadat příkaz CLUSSDR, poté příkaz CLUSRCVR. Nevystavujte nejprve příkaz CLUSRCVR, pak příkaz CLUSSDR. Pokud tak učiníte, vytvoříte neověřené kanály, které mají stav STOPPED. Poté je třeba vydat příkaz START CHANNEL pro zotavení zastavených kanálů; například START CHANNEL(CHNSTORE.CHICAGO).

Zobrazí se zprávy označující, že pro klastr CHNSTORE neexistují žádná úložiště.

Pokud jste neodebrali fronty klastru, jak je popsáno v kroku 1, udělejte to nyní.

5. Zastavit kanály klastru.

V systému CHICAGO zastavte kanály klastru s následujícími příkazy:

```
STOP CHANNEL(CHNSTORE.CHICAGO2)
STOP CHANNEL(CHNSTORE.CHICAGO)
```

6. Opakujte kroky 4 a 5 pro každého správce front v klastru.

7. Zastavte kanály klastru a potom odeberte všechny definice pro kanály klastru a fronty klastru z každého správce front.

8. Volitelné: Vymažte informace o klastru uložené v mezipaměti, které má správce front.

Přestože správci front již nejsou členy klastru, každá z nich uchovává kopii informací o klastru v mezipaměti. Chcete-li tato data odebrat, prohlédněte si úlohu [“Obnova správce front do stavu před klastrem”](#) na stránce 289.

9. Nahrazení definic vzdálených front pro produkt INVENTQ

Aby mohla síť pokračovat ve funkci, nahraďte definici vzdálené fronty pro produkt INVENTQ v každém správci front.

10. Vytoč klastr.

Vymažte všechny definice front nebo kanálů, které již nejsou vyžadovány.

Související úlohy

[Přidání nového propojeného klastru](#)

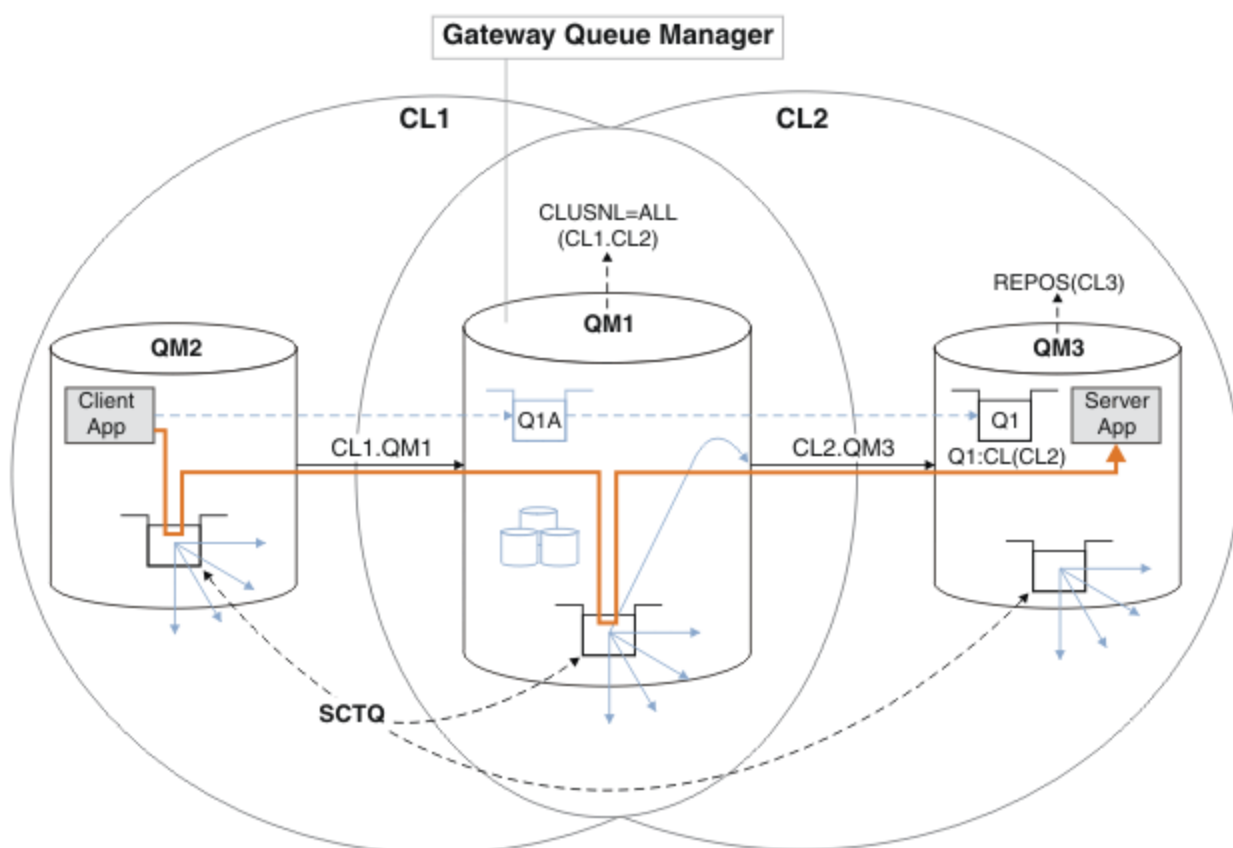
[Přidejte nový klastr, který bude sdílet některé správce front s existujícím klastrem.](#)

Vytvoření dvou překrývajících se klastrů se správcem front brány

Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv do jedné aplikace ze zpráv do jiných aplikací v klastru.

Informace o této úloze

Příklad konfigurace klastru, který se používá pro ilustraci izolování provozu zpráv klastru, je zobrazen v Obrázek 48 na stránce 263. Tento příklad je popsán v tématu [Klastrování: Izolace aplikací pomocí více přenosových front klastru](#).



Obrázek 48. Aplikace Client-server implementovaná do rozbočovače a mluvila s architekturou pomocí klastrů produktu IBM MQ .

Chcete-li učinit z počtu kroků sestavení příkladu tak málo, jak je to možné, konfigurace se chová jednoduše, spíše než realistická. Příklad může představovat integraci dvou klastrů vytvořených dvěma oddělenými organizacemi. Další realistický scénář naleznete v tématu [Klastrování: Plánování konfigurace přenosových front klastru](#).

Při vytváření klastrů postupujte podle kroků. Klastry se používají v následujících příkladech, jak izolovat provoz zpráv z aplikace klienta do serverové aplikace.

Instrukce přidávají dvojici dalších správců front tak, aby každý klaster měl dvě úložiště. Správce front brány se nepoužívá jako úložiště z důvodů výkonu.

Postup

1. Vytvořte a spusťte správce front QM1, QM2, QM3, QM4, QM5.

```

crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE QM n
stmqmq QmgrName

```

Poznámka: QM4 a QM5 jsou úplná úložiště úplných úložišť pro klastry.

2. Definujte a spusťte listenery pro každého správce front.

```

*... On QM n
DEFINE LISTENER(TCP141 n) TRPTYPE(TCP) IPADDR(hostname) PORT(141 n) CONTROL(QMGR) REPLACE
START LISTENER(TCP141 n)

```

3. Vytvořte seznam názvů klastrů pro všechny klastry.

```

*... On QM1
DEFINE NAMELIST(ALL) NAMES(CL1, CL2) REPLACE

```

4. Zhotovte úplná úložiště QM2 a QM4 pro úplná úložiště CL1, QM3 a QM5 pro CL2.

a) Pro CL1:

```

*... On QM2 and QM4
ALTER QMGR REPOS(CL1) DEFCLXQ(SCTQ)

```

b) Pro CL2:

```

*... On QM3 and QM5
ALTER QMGR REPOS(CL2) DEFCLXQ(SCTQ)

```

5. Přidejte kanály odesílatele klastru a příjemce klastru pro každého správce front a klastru.

Spusťte následující příkazy na QM2, QM3, QM4 a QM5, kde *c*, *na m* hodnoty zobrazené v [Tabulka 25](#) na stránce 264 pro každého správce front:

Tabulka 25. Hodnoty parametrů pro vytvoření klastrů 1 a 2

Správce front	Klaster <i>c</i>	Jiné úložiště <i>n</i>	Toto úložiště <i>m</i>
QM2	1	4	2
QM4	1	2	4
QM3	2	5	3
QM5	2	3	5

```

*... On QM m
DEFINE CHANNEL(CL c.QM n) CHLTYPE(CLUSSDR) CONNAME('localhost(141 n)') CLUSTER(CL c) REPLACE
DEFINE CHANNEL(CL c.QM m) CHLTYPE(CLUSRCVR) CONNAME('localhost(141 m)') CLUSTER(CL c) REPLACE

```

6. Přidejte správce front brány QM1 do každého z klastrů.

```

*... On QM1
DEFINE CHANNEL(CL1.QM2) CHLTYPE(CLUSSDR) CONNAME('localhost(1412)') CLUSTER(CL1) REPLACE
DEFINE CHANNEL(CL1.QM1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1411)') CLUSTER(CL1) REPLACE
DEFINE CHANNEL(CL2.QM3) CHLTYPE(CLUSSDR) CONNAME('localhost(1413)') CLUSTER(CL2) REPLACE
DEFINE CHANNEL(CL2.QM1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1411)') CLUSTER(CL2) REPLACE

```

7. Přidejte lokální frontu Q1 do správce front QM3 v klastru CL2.

```

*... On QM3
DEFINE QLOCAL(Q1) CLUSTER(CL2) REPLACE

```


8. Přidejte alias klastrovaného správce front Q1A do správce front brány.

```
*... On QM1
DEFINE QALIAS(Q1A) CLUSNL(ALL) TARGET(Q1) TARGTYPE(Queue) DEFBIND(NOTFIXED) REPLACE
```

Poznámka: Aplikace, které používají alias správce front ve všech ostatních správci front, ale QM1, musí při otevření fronty aliasů zadat DEFBIND(NOTFIXED) . Hodnota **DEFBIND** určuje, zda jsou informace o směrování v záhlaví zprávy opraveny při otevření fronty aplikací. Je-li nastaveno na výchozí hodnotu OPEN, jsou zprávy směrovány do produktu Q1@QM1. Q1@QM1 neexistuje, takže zprávy z jiných správců front končí ve frontě zablokovaných dopisů. Nastavením atributu fronty na DEFBIND(NOTFIXED), aplikace jako **amqspu**t, které se standardně nastaví na nastavení fronty **DEFBIND**, se bude chovat správným způsobem.

9. Přidejte definice aliasu správce front klastru pro všechny správce front s klastry do správce front brány, QM1.

```
*... On QM1
DEFINE QREMOTE(QM2) RNAME(' ') RQMNAME(QM2) CLUSNL(ALL) REPLACE
DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSNL(ALL) REPLACE
```

Tip: Definice alias správce front ve zprávách o přenosu správce front brány, které odkazují na správce front v jiném klastru, najdete v tématu [Klastrované aliasy správce front](#).

Jak pokračovat dále

1. Otestujte definici aliasu fronty odesláním zprávy z produktu QM2 do produktu Q1 v produktu QM3 s použitím definice aliasu fronty Q1A.
 - a. Spustte ukázkový program **amqspu**t na QM2 a zadejte zprávu.

```
C:\IBM\MQ>amqspu Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

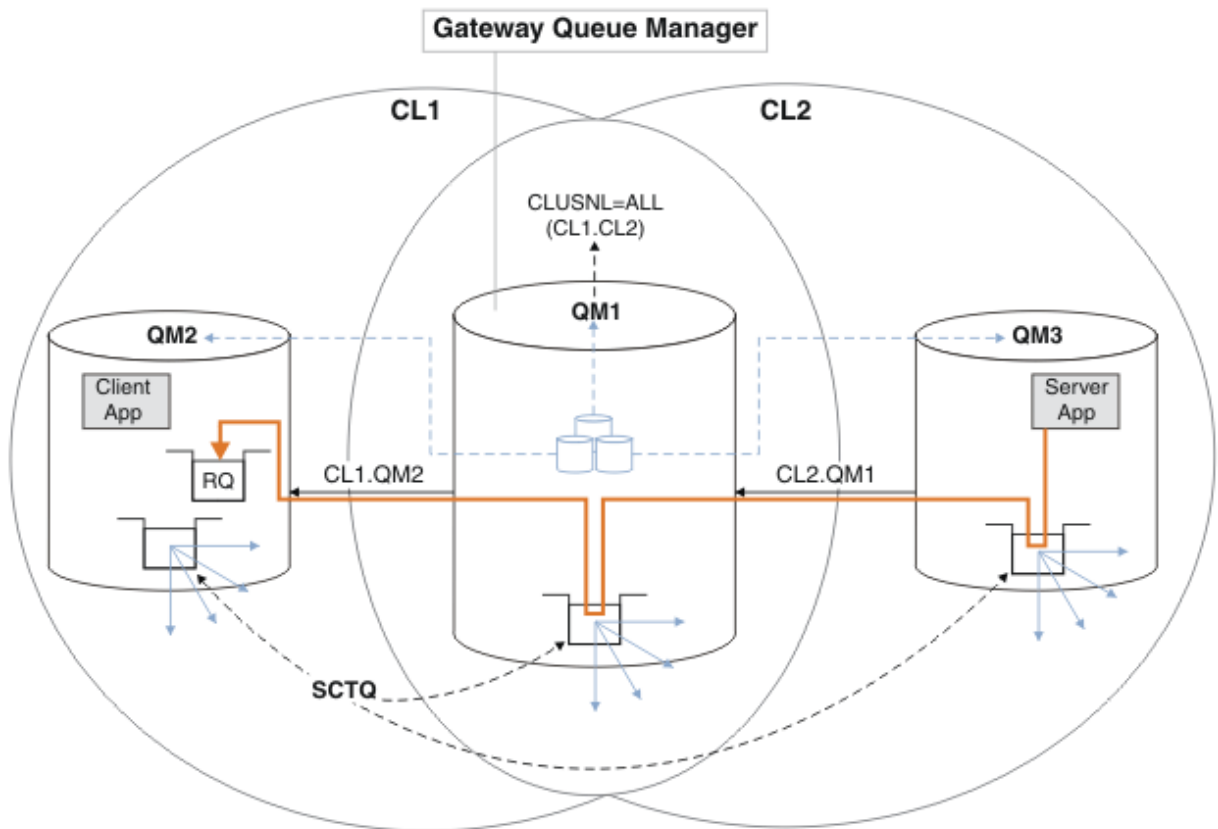
Sample AMQSPUT0 end
```

- b. Spuštěním ukázkového programu **amqsge**t získáte zprávu z produktu Q1 v systému QM3 .

```
C:\IBM\MQ>amqsge Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

2. Otestujte definice aliasů správce front odesláním zprávy požadavku a přijetím zprávy s odpovědí do fronty dočasných dynamických odpovědí.

Diagram zobrazuje cestu, která byla přijata zprávou odpovědi zpět do dočasné dynamické fronty, která se nazývá RQ. Serverová aplikace připojená k produktu QM3 otevře frontu odpovědí s použitím názvu správce front QM2. Název správce front QM2 je definován jako alias klastrovaného správce front v systému QM1. QM3 směruje zprávu odpovědi na QM1. QM1 směruje zprávu do QM2.



Obrázek 49. Použití aliasu správce front k vrácení zprávy odpovědi do jiného klastru

Způsob práce směrování je následující. Každý správce front v každém klastru má definici aliasu správce front v produktu QM1. Aliasy jsou klastrované ve všech klastrech. Šedé přerušované šipky z každého z aliasů do správce front ukazují, že každý alias správce front je převeden na skutečného správce front alespoň v jednom z klastrů. V tomto případě je alias produktu QM2 klastrovaný v klastru CL1 a v produktu CL2a je interpretován jako skutečný správce front QM2 v produktu CL1. Serverová aplikace vytvoří zprávu s odpovědí pomocí odpovědi na název fronty RQa odpoví na název správce front QM2. Zpráva je směrována na QM1, protože definice aliasu správce front QM2 je definována na QM1 v klastru CL2 a správce front QM2 se nenachází v klastru CL2. Vzhledem k tomu, že zprávu nelze odeslat cílovému správci front, bude odeslána správci front s definicí aliasu.

QM1 umístí zprávu do přenosové fronty klastru v systému QM1 for transferal do QM2. Produkt QM1 směruje zprávu do produktu QM2, protože definice aliasu správce front v produktu QM1 for QM2 definuje QM2 jako skutečného cílového správce front. Definice není cyklická, protože definice aliasů se mohou odkazovat pouze na skutečné definice; alias nemůže odkazovat sám na sebe. Skutečná definice je interpretována produktem QM1, protože se oba QM1 a QM2 nacházejí ve stejném klastru, CL1. Produkt QM1 najde informace o připojení pro produkt QM2 z úložiště pro produkt CL1a směruje zprávu do produktu QM2. Aby mohla být zpráva přesměrována produktem QM1, serverová aplikace musí mít otevřenou frontu odpovědi s volbou DEFBIND nastavenou na MQBND_BIND_NOT_FIXED. Pokud měla aplikace serveru otevřenou frontu odpovědi s volbou MQBND_BIND_ON_OPEN, zpráva není přesměrována a ukončí se ve frontě nedoručených zpráv.

- a. Vytvořte klastrovanou frontu požadavků se spouštěčem v systému QM3.

```
*... On QM3
DEFINE QLOCAL(QR) CLUSTER(CL2) TRIGGER INITQ(SYSTEM.DEFAULT.INITIATION.QUEUE)
PROCESS(ECHO) REPLACE
```

b. Vytvořte definici aliasu klastrované fronty produktu QR ve správci front brány QM1.

```
*... On QM1
DEFINE QALIAS(QRA) CLUSNL(ALL) TARGET(QR) TARGTYPE(Queue) DEFBIND(NOTFIXED) REPLACE
```

c. Vytvořte definici procesu ke spuštění ukázkového programu echo **amqsech** v systému QM3.

```
*... On QM3
DEFINE PROCESS(ECHO) APPLICID(AMQSECH) REPLACE
```

d. Vytvořte modelovou frontu na QM2 pro ukázkový program **amqsreq**, abyste vytvořili dočasnou-dynamickou frontu odpovědí.

```
*... On QM2
DEFINE QMODEL(SYSTEM.SAMPLE.REPLY) REPLACE
```

e. Otestujte definici aliasu správce front odesláním požadavku z produktu QM2 do produktu QR v produktu QM3 s použitím definice aliasu fronty QRA.

i) Spusťte program pro monitorování spouštěčů v systému QM3.

```
runmqtrm -m QM3
```

Výstup je

```
C:\IBM\MQ>runmqtrm -m QM3
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.
01/02/2012 16:17:15: IBM MQ trigger monitor started.
```

```
-----
01/02/2012 16:17:15: Waiting for a trigger message
```

ii) Spusťte ukázkový program **amqsreq** na QM2 pro vložení požadavku a čekání na odpověď.

```
C:\IBM\MQ>amqsreq QRA QM2
Sample AMQSREQ0 start
server queue is QRA
replies to 4F2961C802290020
A request message from QM2 to QR on QM3

response <A request message from QM2 to QR on QM3>
no more replies
Sample AMQSREQ0 end
```

Související úlohy

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 240

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Související informace

[Řízení přístupu a více přenosových front klastru](#)

[Klastrování: izolace aplikace pomocí více přenosových front klastru](#)

[Klastrování: Plánování konfigurace přenosových front klastru](#)

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

Než začnete

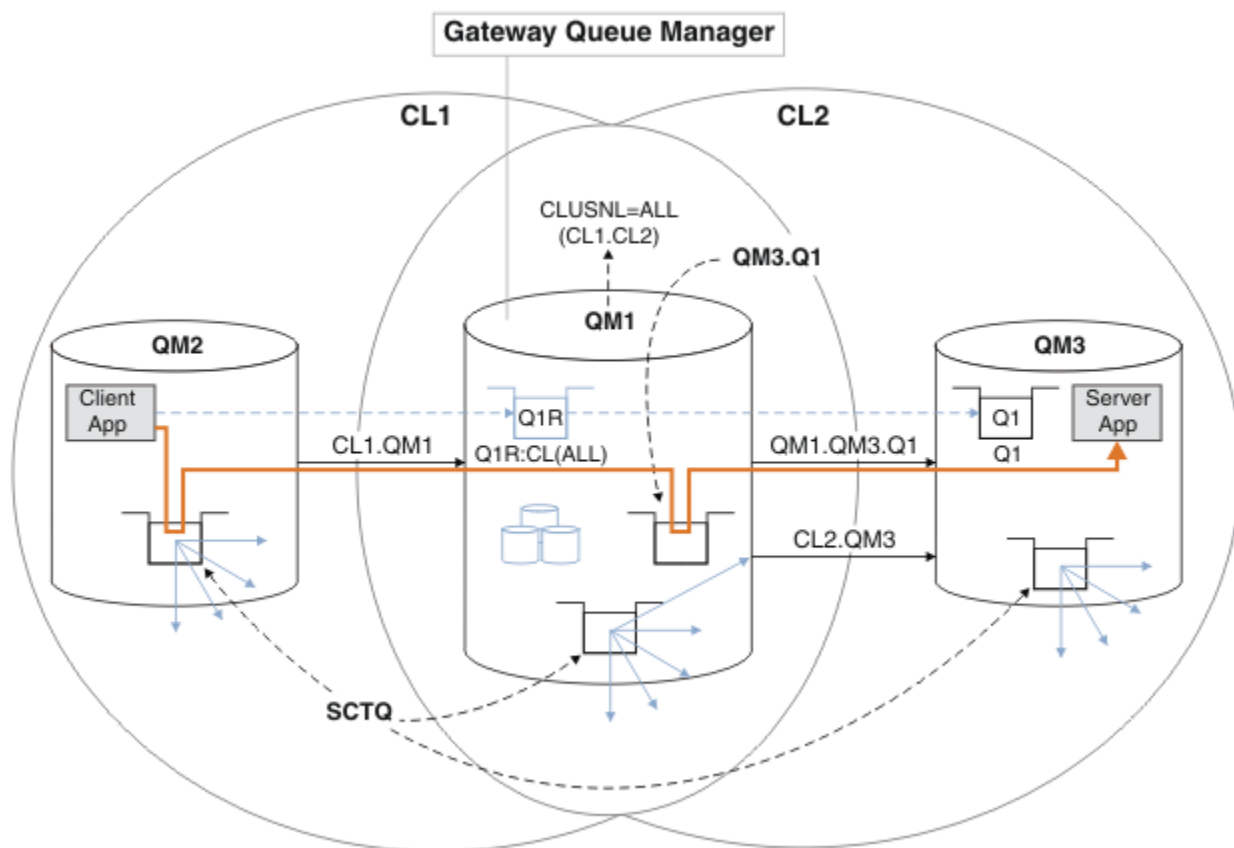
Sestavte překrývající se klastry zobrazené v aplikaci Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 263 podle kroků uvedených v této úloze.

Informace o této úloze

Řešení používá distribuované řazení do fronty k oddělení zpráv pro aplikaci Server App od jiných přenosů zpráv ve správci front brány. Chcete-li převést zprávy do jiné přenosové fronty a do jiného kanálu, je třeba definovat definici klastrované vzdálené fronty v produktu QM1. Definice vzdálené fronty musí obsahovat odkaz na konkrétní přenosovou frontu, která ukládá zprávy pouze pro produkt Q1 v systému QM3. V produktu Obrázek 50 na stránce 268 je alias fronty klastru Q1A doplněn o definici vzdálené fronty Q1Ra je přidána přenosová fronta a odesílací kanál.

V tomto řešení jsou všechny odpovědi vráceny pomocí obvyklých SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Výhodou tohoto řešení je to, že je snadné oddělit provoz pro více cílových front na stejném správci front, ve stejném klastru. Nevýhodou řešení je to, že nelze použít vyrovnávání pracovní zátěže klastru mezi více kopiemi produktu Q1 v různých správci front. Chcete-li tuto nevýhodu překonat, viz “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 270. Také musíte spravovat přepínač z jedné přenosové fronty do druhé.



Obrázek 50. Client-server aplikace implementovaná do rozbočovače a promluvíla architekturu klastru pomocí definic vzdálených front

Postup

1. Vytvořit kanál pro oddělení provozu zpráv produktu Q1 ze správce front brány
 - a) Vytvořte kanál odesílatele ve správci front brány, QM1, do cílového správce front, QM3.

```
DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(SDR) CONNAME(QM3HostName(1413)) XMITQ(QM3.Q1) REPLACE
```

b) Vytvořte přijímací kanál na cílovém správci front, QM3.

```
DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(RCVR) REPLACE
```

2. Vytvoření přenosové fronty ve správci front brány pro přenos zpráv do produktu Q1

```
DEFINE QLOCAL(QM3.Q1) USAGE(XMITQ) REPLACE  
START CHANNEL(QM1.QM3.Q1)
```

Probíhá spouštění kanálu, který je přidružen k přenosové frontě, asociuje přenosovou frontu s kanálem. Kanál se spustí automaticky, jakmile je k kanálu přidružena přenosová fronta.

3. Doplňte definici aliasu klastrované fronty pro produkt Q1 ve správci front brány s definicí klastrované vzdálené fronty.

```
DEFINE QREMOTE CLUSNL(ALL) RNAME(Q1) RQMNAME(QM3) XMITQ(QM3.Q1) REPLACE
```

Jak pokračovat dále

Otestujte konfiguraci odesláním zprávy do produktu Q1 v umístění QM3 z produktu QM2 pomocí definice vzdálené fronty klastrované fronty Q1R ve správci front brány QM1.

1. Spusťte ukázkový program **amqspuť** na QM2 a zadejte zprávu.

```
C:\IBM\MQ>amqspuť Q1R QM2  
Sample AMQSPUť0 start  
target queue is Q1R  
Sample request message from QM2 to Q1 using Q1R
```

```
Sample AMQSPUť0 end
```

2. Spuštěním ukázkového programu **amqsget** získáte zprávu z produktu Q1 v systému QM3 .

```
C:\IBM\MQ>amqsget Q1 QM3  
Sample AMQSGET0 start  
message <Sample request message from QM2 to Q1 using Q1R>  
no more messages  
Sample AMQSGET0 end
```

Související úlohy

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

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

Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

[“Přidání správce front do klastru: samostatné přenosové fronty”](#) na stránce 240

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Související informace

[Klastrování: izolace aplikace pomocí více přenosových front klastru](#)

[Klastrování: Plánování konfigurace přenosových front klastru](#)

[Řízení přístupu a více přenosových front klastru](#)

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídatnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

Než začnete

1. Správce front brány musí být na serveru Verze 7.5 nebo novějším.
2. Sestavte překrývající se klastry zobrazené v aplikaci [Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány”](#) na stránce 263 podle kroků uvedených v této úloze.

Informace o této úloze

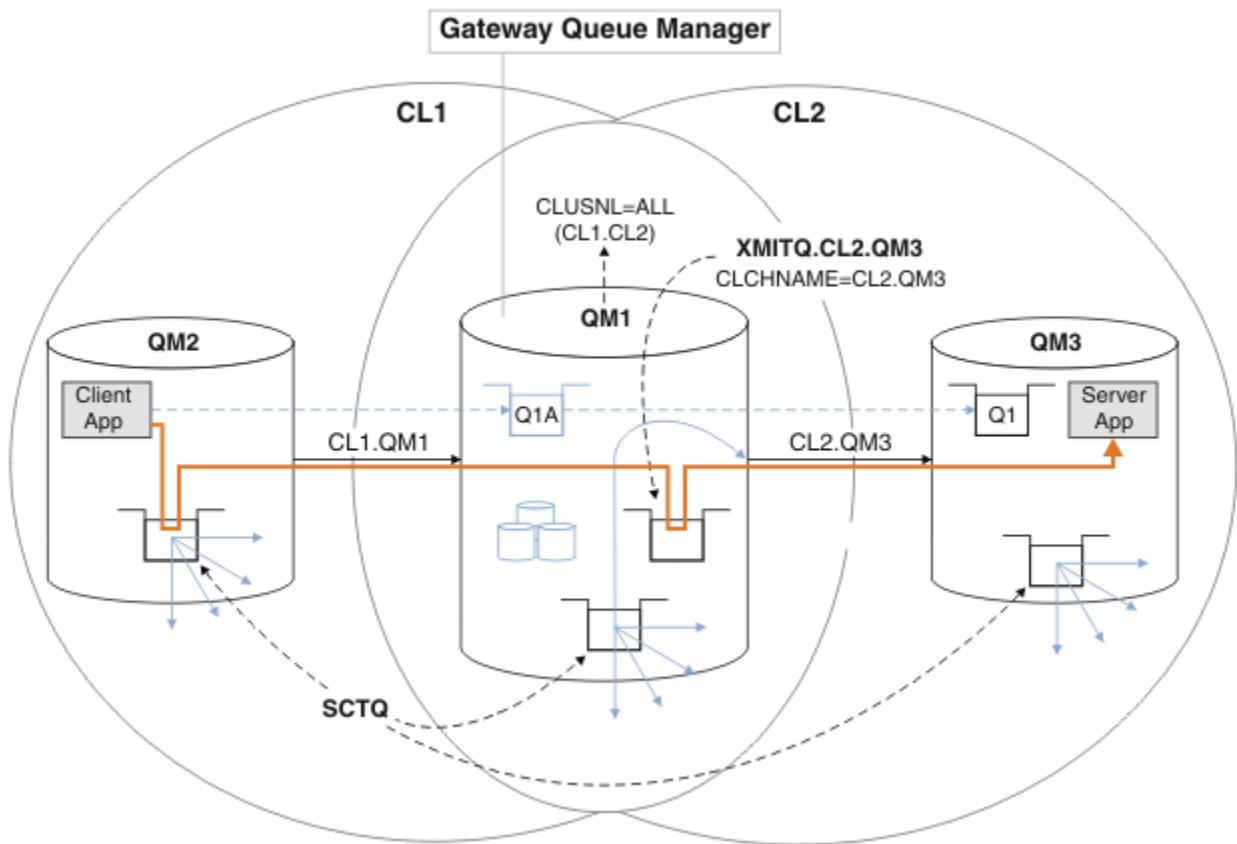
Na správci front brány, QM1, přidejte přenosovou frontu a nastavte její atribut fronty CLCHNAME. Nastavte parametr CLCHNAME na název přijímacího kanálu klastru v systému QM3 . viz [Obrázek 51](#) na stránce 271.

Toto řešení má řadu výhod oproti řešení popsanému v příručce [“Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány”](#) na stránce 267:

- Vyžaduje méně dodatečných definic.
- Podporuje vyvážení pracovní zátěže mezi více kopiemi cílové fronty, Q1, v různých správcích front ve stejném klastru, CL2.
- Správce front brány se automaticky přepne na novou konfiguraci, jakmile se kanál restartuje, aniž by došlo k ztrátě zpráv.
- Správce front brány pokračuje v předávání zpráv ve stejném pořadí, v jakém byla přijata. To znamená, i když se přepnutí provádí se zprávami pro frontu Q1 v QM3 stále na SYSTEM . CLUSTER . TRANSMIT . QUEUE.

Konfigurace k izolování provozu zpráv klastru v produktu [Obrázek 51](#) na stránce 271 nevedla k tomu, že by byla velká izolace provozu jako konfigurace pomocí [vzdálených front v produktu “Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány”](#) na stránce 267. Pokud správce front QM3 v produktu CL2 hostí řadu různých front klastru a aplikací serveru, všechny tyto fronty sdílejí kanál klastru, CL2 . QM3, připojující se QM1 k QM3. Další toky jsou ilustrovány v [Obrázek 51](#) na stránce 271 se šedou šipkou představující potenciální provoz zpráv klastru z SYSTEM . CLUSTER . TRANSMIT . QUEUE do kanálu odesílatele klastru CL2 . QM3.

Opravem je omezení správce front o hostování jedné fronty klastru v konkrétním klastru. Je-li správce front již hostitelem určitého počtu front klastru, je třeba toto omezení splnit, musíte buď vytvořit jiného správce front, nebo vytvořit jiný klastr. Viz téma [“Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány”](#) na stránce 273.



Obrázek 51. Client-server aplikace implementovaná do rozbočovače a promluvila o architektuře s použitím další přenosové fronty klastru.

Postup

1. Vytvořte další přenosovou frontu klastru pro odesílací kanál klastru CL2 . QM3 ve správci front brány QM1.

```
*... on QM1
DEFINE QLOCAL(XMITQ.CL2.QM3) USAGE(XMITQ) CLCHNAME(CL2.QM3)
```

2. Přepněte na použití přenosové fronty XMITQ . CL2 . QM3.
 - a) Zastavte odesílací kanál klastru CL2 . QM3.

```
*... On QM1
STOP CHANNEL(CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

AMQ8019: Stop IBM MQ channel accepted.

- b) Zkontrolujte, zda je kanál CL2 . QM3 zastaven.

Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou **FORCE** . Příklad nastavení volby **FORCE** by byl v případě, že se kanál nezastaví, a ostatní správce front nelze restartovat, aby se kanál synchronizoval.

```
*... On QM1
start
```

Odezva je souhrnem stavu kanálu.

```
AMQ8417: Display Channel Status details.  
CHANNEL (CL2.QM3)           CHLTYPE (CLUSSDR)  
CONNNAME (127.0.0.1(1413))  CURRENT  
RQMNAME (QM3)              STATUS (STOPPED)  
SUBSTATE (MQGET)           XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

c) Spustte kanál, CL2.QM3.

```
*... On QM1  
START CHANNEL (CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

d) Zkontrolujte, zda je kanál spuštěn.

```
*... On QM1  
DISPLAY CHSTATUS (CL2.QM3)
```

Odezva je souhrnem stavu kanálu:

```
AMQ8417: Display Channel Status details.  
CHANNEL (CL2.QM3)           CHLTYPE (CLUSSDR)  
CONNNAME (127.0.0.1(1413))  CURRENT  
RQMNAME (QM3)              STATUS (RUNNING)  
SUBSTATE (MQGET)           XMITQ (XMITQ.CL2.QM3)
```

e) Zkontrolujte, zda byla přenosová fronta komutována.

Zkontrolujte protokol chyb správce front brány pro zprávu " AMQ7341 Přenosová fronta pro kanál CL2.QM3 je XMITQ.CL2.QM3 ".

Jak pokračovat dále

Otestujte samostatnou přenosovou frontu odesláním zprávy z produktu QM2 do produktu Q1 v produktu QM3 pomocí definice aliasu fronty Q1A

1. Spustte ukázkový program **amqspu**t na QM2 a zadejte zprávu.

```
C:\IBM\MQ>amqspu Q1A QM2  
Sample AMQSPUT0 start  
target queue is Q1A  
Sample request message from QM2 to Q1 using Q1A
```

```
Sample AMQSPUT0 end
```

2. Spuštěním ukázkového programu **amqsge**t získáte zprávu z produktu Q1 v systému QM3 .

```
C:\IBM\MQ>amqsge Q1 QM3  
Sample AMQSGE0 start  
message <Sample request message from QM2 to Q1 using Q1A>  
no more messages  
Sample AMQSGE0 end
```


Související pojmy

[“Práce s přenosovými frontami klastru a odesílacími kanály klastru”](#) na stránce 222

Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru. V libovolném okamžiku je kanál odesílatele klastru asociován s jednou přenosovou frontou. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizováno a transakční.

Související úlohy

[Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány](#)

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

[Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány](#)

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

[Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv](#)

Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

[“Přidání správce front do klastru: samostatné přenosové fronty”](#) na stránce 240

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Související informace

[Řízení přístupu a více přenosových front klastru](#)

[Klastrování: izolace aplikace pomocí více přenosových front klastru](#)

[Klastrování: Plánování konfigurace přenosových front klastru](#)

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

Než začnete

Kroky v úloze jsou napsány tak, aby bylo možné upravit konfiguraci ilustrované v produktu [Obrázek 51](#) na stránce 271.

1. Správce front brány musí být na serveru Verze 7.5 nebo novějším.
2. Sestavte překrývajících se klastry zobrazené v aplikaci [Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ](#) v produktu [“Vytvoření dvou překrývajících se klastrů se správcem front brány”](#) na stránce 263 podle kroků uvedených v této úloze.
3. Chcete-li vytvořit řešení bez dalšího klastru, proveďte kroky uvedené v tématu [Obrázek 51](#) na stránce 271 v produktu [“Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány”](#) na stránce 270. Použijte jej jako základ pro kroky v této úloze.

Informace o této úloze

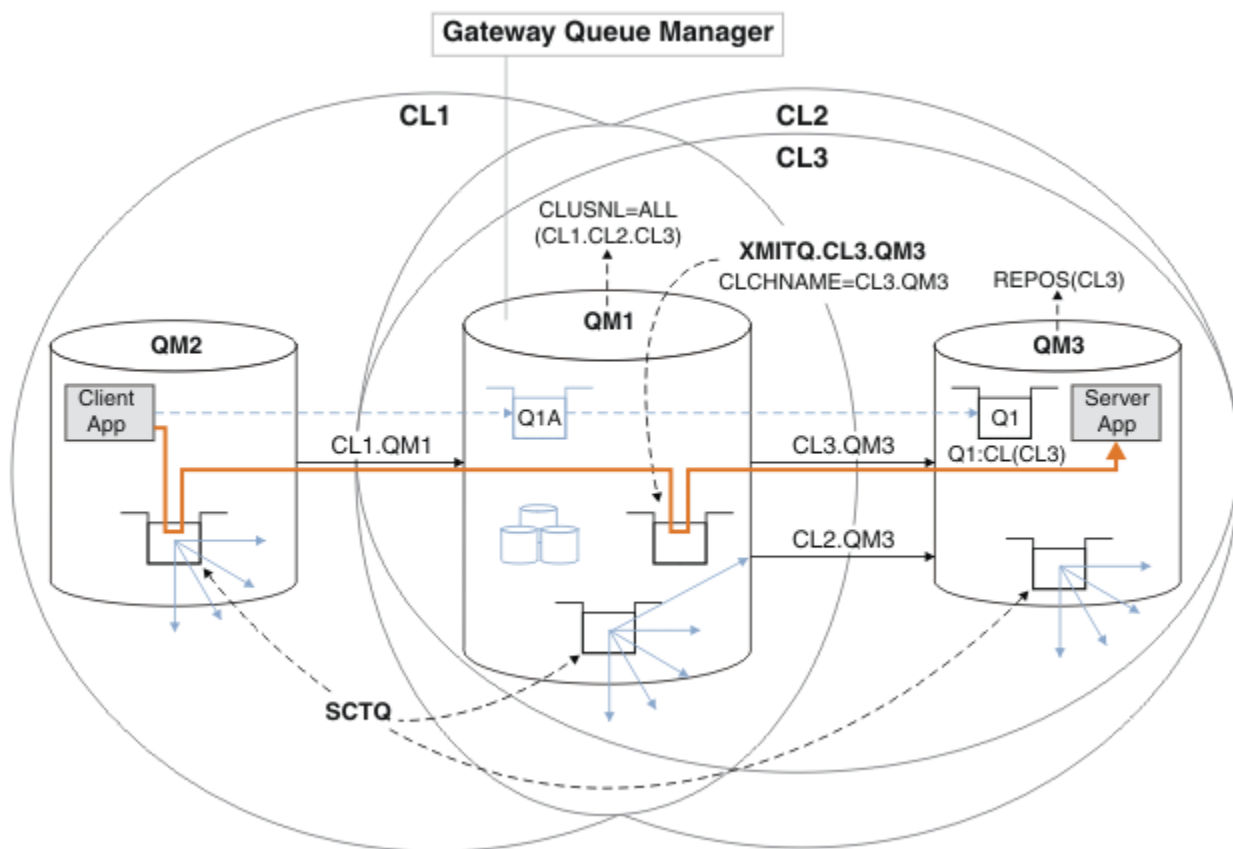
Řešení pro izolování provozu zpráv do jediné aplikace v produktu [“Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány”](#) na stránce 270 funguje, pokud je cílová fronta klastru jedinou frontou klastru ve správci front. Pokud tomu tak není, máte dvě možnosti.

Buď přesuňte frontu na jiného správce front, nebo vytvořte klastr, který izoluje danou frontu od jiných front klastru ve správci front.

Tato úloha vás provede kroky k přidání klastru k izolaci cílové fronty. Klastr je přidán pouze pro tento účel. V praxi se při navrhování klastrů a schémat pojmenování klastrů postupně přibližte k úloze izolace určitých aplikací. Přidání klastru pokaždé, když fronta vyžaduje izolaci, může skončit s mnoha klastry, které se mají spravovat. V této úloze změníte konfiguraci v produktu “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 270 přidáním klastru CL3 za účelem izolace Q1 v systému QM3. Aplikace budou pokračovat ve zpracování po celou dobu změny.

Nové a změněné definice jsou v produktu Obrázek 52 na stránce 274 zvýrazněny. Souhrn změn je následující: Vytvoření klastru, což znamená, že musíte také vytvořit nové úplné úložiště klastru. V příkladu QM3 se vytvoří jedno z úplných úložišť pro produkt CL3. Chcete-li přidat správce front brány do nového klastru, vytvořte odesílací kanály klastru a příjemce klastru pro produkt QM1. Změňte definici Q1 tak, aby se přepnul na CL3. Upravte seznam názvů klastru ve správci front brány a přidejte přenosovou frontu klastru pro použití nového kanálu klastru. Nakonec přepněte alias fronty Q1A do nového seznamu názvů klastru.

Produkt IBM MQ nemůže přenášet zprávy z přenosové fronty XMITQ . CL2 . QM3 , které jste přidali v “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 270 do nové přenosové fronty XMITQ . CL3 . QM3, automaticky. Může přenášet zprávy automaticky pouze v případě, že obě přenosové fronty jsou obsluhovány stejným odesílacím kanálem klastru. Místo toho úloha popisuje jeden způsob, jak ručně provést přepnutí, což by mohlo být vhodné pro vás. Po dokončení přenosu máte možnost vrátit se k použití výchozí přenosové fronty klastru pro další fronty klastru CL2 v systému QM3. Nebo můžete pokračovat v používání produktu XMITQ . CL2 . QM3. Rozhodnete-li se vrátit se k výchozí přenosové frontě klastru, správce front brány pro vás automaticky spravuje přepínač.



Obrázek 52. Použití dalšího klastru k oddělení provozu zpráv ve správci front brány, který vede k jednomu z více front klastru ve stejném správci front

Postup

1. Upravte správce front QM3 a QM5 tak, aby byla úložiště pro produkty CL2 i CL3.

Chcete-li vytvořit správce front jako člena více klastrů, je třeba použít seznam názvů klastrů k identifikaci klastrů, jejichž členem je.

```
*... On QM3 and QM5
DEFINE NAMELIST(CL23) NAMES(CL2, CL3) REPLACE
ALTER QMGR REPOS(' ') REPOSNL(CL23)
```

2. Definujte kanály mezi správci front QM3 a QM5 for CL3.

```
*... On QM3
DEFINE CHANNEL(CL3.QM5) CHLTYPE(CLUSSDR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE
DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSRCVR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE

*... On QM5
DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSSDR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE
DEFINE CHANNEL(CL3.QM5) CHLTYPE(CLUSRCVR) CONNAME('localhost(1415)') CLUSTER(CL3) REPLACE
```

3. Přidejte správce front brány do produktu CL3.

Přidejte správce front brány přidáním QM1 do produktu CL3 jako dílčího úložiště. Vytvořte dílčí úložiště tak, že přidáte kanály odesílatele klastru a příjemce klastru do produktu QM1.

Také přidejte CL3 do seznamu názvů všech klastrů připojených ke správci front brány.

```
*... On QM1
DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSSDR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE
DEFINE CHANNEL(CL3.QM1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1411)') CLUSTER(CL3) REPLACE
ALTER NAMELIST(ALL) NAMES(CL1, CL2, CL3)
```

4. Přidejte přenosovou frontu klastru do správce front brány, QM1, pro zprávy, které se předávají produktu CL3 v systému QM3.

Nejprve zastavte odesílací kanál klastru, který přenáší zprávy z přenosové fronty do doby, než budete připraveni přepnout přenosové fronty.

```
*... On QM1
DEFINE QLOCAL(XMITQ.CL3.QM3) USAGE(XMITQ) CLCHNAME(CL3.QM3) GET(DISABLED) REPLACE
```

5. Vysune zprávy z existující přenosové fronty klastru XMITQ.CL2.QM3.

Tento dílčí postup je určen k uchování pořadí zpráv v produktu Q1 tak, aby odpovídaly pořadí, ve kterém byly obdrženy ve správci front brány. U klastrů není objednávání zpráv plně zaručeno, ale je pravděpodobné. Pokud je vyžadováno zaručené pořadí zpráv, aplikace musí definovat pořadí zpráv, viz [Pořadí, v jakém se zprávy načítají z fronty](#).

- a) Změňte cílovou frontu Q1 na QM3 z CL2 na CL3.

```
*... On QM3
ALTER QLOCAL(Q1) CLUSTER(CL3)
```

- b) Monitorujte XMITQ.CL3.QM3, dokud se do něj nezačne doručovat zprávy.

Zprávy začínají být doručovány do XMITQ.CL3.QM3, když je přepínač Q1 do CL3 šířen do správce front brány.

```
*... On QM1
DISPLAY QUEUE(XMITQ.CL3.QM3) CURDEPTH
```

- c) Monitorujte XMITQ.CL2.QM3, dokud nebude obsahovat žádné zprávy čekající na doručení do Q1 na QM3.

Poznámka: Produkt XMITQ.CL2.QM3 může uchovávat zprávy pro jiné fronty v produktu QM3, které jsou členy produktu CL2. V takovém případě by hloubka nemusela přejít na nulu.

```
*... On QM1
DISPLAY QUEUE(XMITQ.CL2.QM3) CURDEPTH
```

- d) Povolit získání z nové přenosové fronty klastru, XMITQ.CL3.QM3

```
*... On QM1
ALTER QLOCAL(XMITQ.CL3.QM3) GET(ENABLED)
```

6. Odstraňte starou přenosovou frontu klastru, XMITQ.CL2.QM3, pokud již není požadována.

Zprávy pro frontu klastru v produktu CL2 v systému QM3 se vrátí k použití výchozí přenosové fronty klastru ve správci front brány QM1. Výchozí přenosová fronta klastru je buď SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo SYSTEM.CLUSTER.TRANSMIT.CL2.QM3. Který závisí na tom, zda je hodnota atributu správce front **DEFCLXQ** v systému QM1 SCTQ nebo CHANNEL. Správce front přeneše zprávy z produktu XMITQ.CL2.QM3 automaticky, jakmile se spustí odesílací kanál klastru CL2.QM3.

- a) Změňte přenosovou frontu XMITQ.CL2.QM3, aby byla přenosovou frontou klastru, aby byla normální přenosovou frontou.

Tím dojde k přerušení přidružení přenosové fronty k libovolným odesílacím kanálům klastru. V odpovědi IBM MQ automaticky přenáší zprávy z XMITQ.CL2.QM3 do výchozí přenosové fronty klastru, když je spuštěn kanál odesílatele klastru. Do té doby jsou zprávy pro CL2 v systému QM3 stále umístěny na XMITQ.CL2.QM3.

```
*... On QM1
ALTER QLOCAL(XMITQ.CL2.QM3) CLCHNAME('')
```

- b) Zastavte odesílací kanál klastru CL2.QM3.

Zastavení a restartování kanálu odesílatele klastru iniciuje přenos zpráv z produktu XMITQ.CL2.QM3 do výchozí přenosové fronty klastru. Zpravidla byste zastavili a spustili kanál ručně, abyste spustili přenos. Přenos se spustí automaticky, pokud se kanál restartuje po vypršení jeho intervalu odpojení.

```
*... On QM1
STOP CHANNEL(CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8019: Stop IBM MQ channel accepted.
```

- c) Zkontrolujte, zda je kanál CL2.QM3 zastaven.

Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou FORCE. Příklad nastavení volby FORCE by byl v případě, že se kanál nezastaví, a ostatní správce front nelze restartovat, aby se kanál synchronizoval.

```
*... On QM1
DISPLAY CHSTATUS(CL2.QM3)
```

Odezva je souhrnem stavu kanálu.

```
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM3)                CHLTYPE(CLUSSDR)
CONNNAME(127.0.0.1(1413))       CURRENT
RQMNAME(QM3)                    STATUS(STOPPED)
SUBSTATE(MQGET)                 XMITQ(XMITQ.CL2.QM3)
```

- d) Spustte kanál, CL2.QM3.

```
*... On QM1
START CHANNEL(CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

e) Zkontrolujte, zda je kanál spuštěn.

```
*... On QM1
DISPLAY CHSTATUS(CL2.QM3)
```

Odezva je souhrnem stavu kanálu:

```
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM3)          CHLTYPE(CLUSSDR)
CONNNAME(127.0.0.1(1413)) CURRENT
RQMNAME(QM3)             STATUS(RUNNING)
SUBSTATE(MQGET)          XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE|CL2.QM3)
```

f) Zkontrolujte protokol chyb správce front brány pro zprávu " AMQ7341 Přenosová fronta pro kanál CL2.QM3 je SYSTEM.CLUSTER.TRANSMIT. QUEUE|CL2.QM3 ".

g) Odstraňte přenosovou frontu klastru, XMITQ.CL2.QM3.

```
*... On QM1
DELETE QLOCAL(XMITQ.CL2.QM3)
```

Jak pokračovat dále

Otestujte odděleně klastrovanou frontu odesláním zprávy z produktu QM2 do produktu Q1 v produktu QM3 s použitím definice aliasu fronty Q1A

1. Spusťte ukázkový program **amqspu**t na QM2 a zadejte zprávu.

```
C:\IBM\MQ>amqspu Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A
```

```
Sample AMQSPUT0 end
```

2. Spuštěním ukázkového programu **amqsget** získáte zprávu z produktu Q1 v systému QM3 .

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

Související pojmy

[“Práce s přenosovými frontami klastru a odesílacími kanály klastru” na stránce 222](#)

Zprávy mezi správci front s klastru se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru. V libovolném okamžiku je kanál odesílatele klastru asociován s jednou přenosovou frontou. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizováno a transakční.

Související úlohy

[Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány](#)

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídatnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

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

Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 240

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Související informace

Řízení přístupu a více přenosových front klastru

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

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

Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

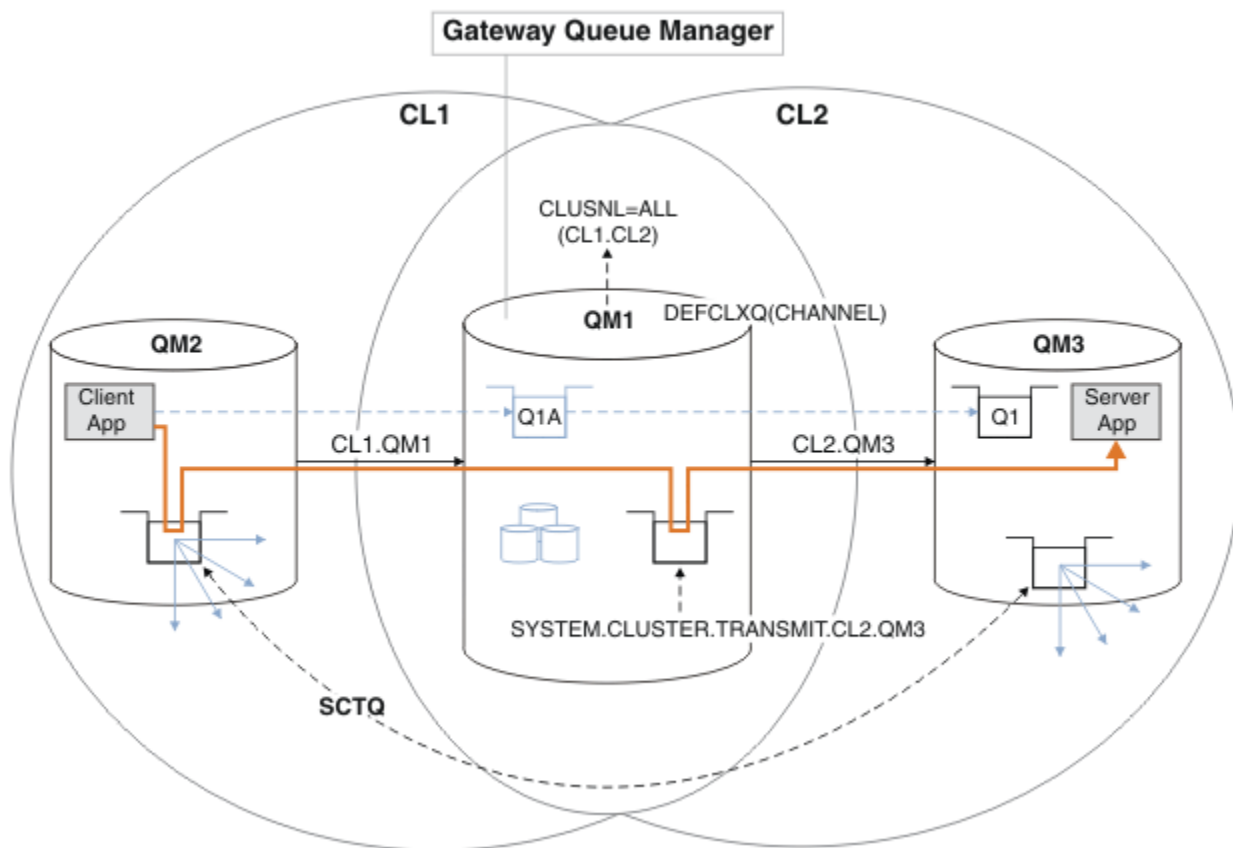
Než začnete

1. Správce front brány musí být na serveru Verze 7.5 nebo novějším.
2. Sestavte překrývajících se klastry zobrazené v aplikaci Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 263 podle kroků uvedených v této úloze.

Informace o této úloze

Chcete-li implementovat architekturu s více frontami klastru, musí být správce front brány na serveru Verze 7.5 nebo novějším. Chcete-li pro správce front brány změnit výchozí typ přenosové fronty klastru, je třeba změnit výchozí typ přenosové fronty klastru. Změňte hodnotu atributu správce front **DEFCLXQ** na QM1 z SCTQ na CHANNEL ; viz Obrázek 53 na stránce 279. Diagram zobrazuje jeden tok zpráv. Pro toky do jiných správců front nebo do jiných klastrů správce front vytvoří další trvalé přenosové fronty dynamického dynamického klastru. Každý odesílací kanál klastru přenáší zprávy z jiné přenosové fronty klastru.

Změna se neprojeví okamžitě, pokud nechcete poprvé připojit správce front brány k klastrům. Úloha zahrnuje kroky pro typický případ správy změny na existující konfiguraci. Chcete-li nastavit správce front tak, aby při prvním připojení ke klastru používal oddělené přenosové fronty klastru, přečtěte si téma “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 240.



Obrázek 53. Client-server aplikace implementovaná do rozbočovače a spoke architektury s oddělenými frontami přenosu klastru ve správci front brány.

Postup

1. Změňte správce front brány tak, aby používal oddělené přenosové fronty klastru.

```
*... On QM1
ALTER QMGR DEFCLXQ(CHANNEL)
```

2. Přepněte na samostatné přenosové fronty klastru.

Libovolný odesílací kanál klastru, který při příštím spuštění nespouští přepínače při použití oddělených přenosových front klastru.

Chcete-li přepnout spuštěné kanály, buď znovu spusťte správce front, nebo postupujte takto:

- a) Seznam odesílacích kanálů klastru, které jsou spuštěny s produktem SYSTEM.CLUSTER.TRANSMIT.QUEUE.

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
```

Odezva je seznam sestav stavu kanálu:

```
AMQ8417: Display Channel Status details.
CHANNEL(CL1.QM2)                CHLTYPE(CLUSSDR)
CONNNAME(127.0.0.1(1412))       CURRENT
RQMNAME(QM2)                    STATUS(RUNNING)
SUBSTATE(MQGET)                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
```

```

CHANNEL (CL2.QM3)           CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1413)) CURRENT
RQMNAME (QM3)             STATUS (RUNNING)
SUBSTATE (MQGET)          XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL (CL2.QM5)           CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1415)) CURRENT
RQMNAME (QM5)             STATUS (RUNNING)
SUBSTATE (MQGET)          XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL (CL1.QM4)           CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1414)) CURRENT
RQMNAME (QM4)             STATUS (RUNNING)
SUBSTATE (MQGET)          XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)

```

b) Zastavit spuštěné kanály

Pro každý kanál v seznamu spusťte příkaz:

```

*... On QM1
STOP CHANNEL (ChannelName)

```

Kde *ChannelName* je každý z CL1.QM2, CL1.QM4, CL1.QM3, CL1.QM5.

Odpověď je taková, že příkaz je přijat:

AMQ8019: Stop IBM MQ channel accepted.

c) Monitorovat, které kanály jsou zastavené

```

*... On QM1
DISPLAY CHSTATUS(*) WHERE (XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')

```

Odezva je seznam kanálů, které jsou stále spuštěné, a kanály, které jsou zastaveny:

```

AMQ8417: Display Channel Status details.
CHANNEL (CL1.QM2)           CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1412)) CURRENT
RQMNAME (QM2)             STATUS (STOPPED)
SUBSTATE ( )              XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL (CL2.QM3)           CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1413)) CURRENT
RQMNAME (QM3)             STATUS (STOPPED)
SUBSTATE ( )              XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL (CL2.QM5)           CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1415)) CURRENT
RQMNAME (QM5)             STATUS (STOPPED)
SUBSTATE ( )              XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL (CL1.QM4)           CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1414)) CURRENT
RQMNAME (QM4)             STATUS (STOPPED)
SUBSTATE ( )              XMITQ (SYSTEM.CLUSTER.TRANSMIT.QUEUE)

```

d) Spusťte každý zastavený kanál.

Tento krok proveďte pro všechny spuštěné kanály. Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou FORCE . Příklad nastavení volby FORCE by byl v případě, že se kanál nezastaví, a ostatní správce front nelze restartovat, aby se kanál synchronizoval.

```
*... On QM1
START CHANNEL (CL2.QM5)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

e) Monitorujte komutované přenosové fronty.

Zkontrolujte protokol chyb správce front brány pro zprávu " AMQ7341 Přenosová fronta pro kanál CL2.QM3 je SYSTEM.CLUSTER.TRANSMIT.QUEUE/CL2.QM3 ".

f) Zkontrolujte, zda již SYSTEM.CLUSTER.TRANSMIT.QUEUE není používáno.

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
DISPLAY QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE) CURDEPTH
```

Odezva je seznam stavových zpráv kanálu a hloubka produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE:

```
AMQ8420: Channel Status not found.
AMQ8409: Display Queue details.
QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE)      TYPE(QLOCAL)
CURDEPTH(0)
```

g) Monitorovat, které kanály jsou spuštěny

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
```

Odezva je seznam kanálů, v tomto případě již je spuštěn s novými výchozími přenosovými frontami klastru:

```
AMQ8417: Display Channel Status details.
CHANNEL (CL1.QM2)                                CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1412))                      CURRENT
RQMNAME (QM2)                                    STATUS (RUNNING)
SUBSTATE (MQGET)
XMITQ (SYSTEM.CLUSTER.TRANSMIT.CL1.QM2)
AMQ8417: Display Channel Status details.
CHANNEL (CL2.QM3)                                CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1413))                      CURRENT
RQMNAME (QM3)                                    STATUS (RUNNING)
SUBSTATE (MQGET)
XMITQ (SYSTEM.CLUSTER.TRANSMIT.CL2.QM3)
AMQ8417: Display Channel Status details.
CHANNEL (CL2.QM5)                                CHLTYPE (CLUSSDR)
CONNNAME (127.0.0.1(1415))                      CURRENT
RQMNAME (QM5)                                    STATUS (RUNNING)
SUBSTATE (MQGET)
XMITQ (SYSTEM.CLUSTER.TRANSMIT.CL2.QM5)
AMQ8417: Display Channel Status details.
CHANNEL (CL1.QM4)                                CHLTYPE (CLUSSDR)
```

```
CONNNAME (127.0.0.1(1414))          CURRENT
RQMNAME (QM4)                       STATUS (RUNNING)
SUBSTATE (MQGET)
XMITQ (SYSTEM.CLUSTER.TRANSMIT.CL1.QM4)
```

Jak pokračovat dále

1. Testujte automaticky definovanou přenosovou frontu klastru odesláním zprávy z produktu QM2 do produktu Q1 v systému QM3a s definicí názvu fronty s definicí aliasu fronty Q1A .
 - a. Spustte ukázkový program **amqspud** na QM2 a zadejte zprávu.

```
C:\IBM\MQ>amqspud Q1A QM2
Sample AMQSPUD0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUD0 end
```

- b. Spuštěním ukázkového programu **amqsget** získáte zprávu z produktu Q1 v systému QM3 .

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

2. Zvažte, zda znovu konfigurovat zabezpečení, a to konfigurací zabezpečení pro fronty klastru na správci front, odkud pocházejí zprávy pro fronty klastru.

Související úlohy

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 240

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Související informace

Řízení přístupu a více přenosových front klastru

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

Odebrání fronty klastru ze správce front

Zakažte frontu INVENTQ v Torontu. Odešle všechny zprávy soupisu do New Yorku a odstraní frontu INVENTQ v Torontu, když je prázdná.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastř INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front, který je hostitelem fronty” na stránce 245. Obsahuje čtyři správce front. LONDON a NEWYORK obsahují úplná úložiště. PARIS a TORONTO obsahují dílčí úložiště. Aplikace inventáře se spouští na systémech v New Yorku a Torontu a je řízena přijetím zpráv ve frontě INVENTQ .
- Vzhledem ke snížení pracovní zátěže již nechcete spouštět aplikaci inventáře v Torontu. Chcete zakázat frontu INVENTQ , jejímž hostitelem je správce front TORONTO, a v produktu NEWYORK mají zprávy kanálu TORONTO ke frontám INVENTQ .
- Síťová konektivita existuje mezi všemi čtyřmi systémy.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li odebrat frontu klastru, postupujte takto.

Postup

1. Označuje, že fronta již není k dispozici.

Chcete-li odebrat frontu z klastru, odeberte název klastru z definice lokální fronty. Pozměnit INVENTQ na TORONTO tak, aby nebyla přístupná ze zbytku klastru:

```
ALTER QLOCAL(INVENTQ) CLUSTER(' ')
```

2. Zkontrolujte, zda již fronta není k dispozici.

Ve správci front úplného úložiště, buď LONDON nebo NEWYORK, zkontrolujte, že fronta již není hostitelem správce front TORONTO zadáním následujícího příkazu:

```
DIS QCLUSTER (INVENTQ)
```

Příkaz TORONTO není uveden ve výsledcích, pokud byl příkaz ALTER úspěšně dokončen.

3. Zakažte frontu.

Zakažte frontu INVENTQ na TORONTO tak, aby do ní nebyly zapsány žádné další zprávy:

```
ALTER QLOCAL(INVENTQ) PUT(DISABLED)
```

Nyní probíhá odesílání zpráv do této fronty pomocí příkazu MQOO_BIND_ON_OPEN do fronty nedoručených zpráv. Je třeba ukončit všechny aplikace, aby byly explicitně odesílány zprávy do fronty v tomto správci front.

4. Monitorujte frontu, dokud není prázdná.

Monitorujte frontu pomocí příkazu DISPLAY QUEUE , uveďte atributy IPPROCS, OPPOCSa CURDEPTH, nebo použijte příkaz WRKMQMSTS na IBM i. Když je počet vstupních a výstupních procesů a aktuální hloubka queuesare nula, je fronta prázdná.

5. Monitorujte kanál, abyste se ujistili, že neexistují žádné nejisté zprávy.

Chcete-li se ujistit, že kanál INVENTORY . TORONTO neobsahuje žádné nejisté zprávy, sledujte kanál odesílatele klastru s názvem INVENTORY . TORONTO v každém z ostatních správců front. Zadejte příkaz DISPLAY CHSTATUS se zadáním parametru INDOUBT z každého správce front:

```
DISPLAY CHSTATUS(INVENTORY.TORONTO) INDOUBT
```

Pokud existují nějaké neověřené zprávy, musíte je vyřešit, než budete pokračovat. Například můžete zkusit vydat příkaz kanálu RESOLVE nebo zastavit a restartovat kanál.

6. Vymažte lokální frontu.

Jste-li spokojeni s tím, že v produktu TORONTO nejsou k dispozici žádné další zprávy, které by bylo možné doručit do aplikace soupisu, můžete frontu odstranit:

```
DELETE QLOCAL(INVENTQ)
```

7. Nyní můžete odebrat aplikaci soupisu ze systému v Torontu

Odebráním aplikace se vyhnete duplikaci a šetří místo na systému.

Výsledky

Klastr, který je nastaven touto úlohou, je stejný jako u nastavení předchozí úlohy. Rozdíl je v tom, že fronta INVENTQ již není ve správci front TORONTO k dispozici.

Když jste v kroku 1 zanesli frontu ze služby, správce front produktu TORONTO odeslal zprávu do dvou správců front úplného úložiště. Informovali je o změně stavu. Správci front úplného úložiště předávají tyto informace ostatním správcům front v klastru, kteří požadovali aktualizace informací týkajících se konzoly INVENTQ.

Když správce front vloží zprávu do fronty produktu INVENTQ, aktualizované dílčí úložiště označuje, že fronta INVENTQ je k dispozici pouze ve správci front NEWYORK. Zpráva se odešle do správce front produktu NEWYORK.

Jak pokračovat dále

V této úloze byla pouze jedna fronta pro odebrání a pouze jeden klastr, ze kterého se má odebrat.

Předpokládejme, že existuje mnoho front odkazujících na seznam názvů obsahující mnoho názvů klastrů. Například správce front produktu TORONTO nemusí být hostitelem pouze produktu INVENTQ, ale také PAYROLLQ, SALESQ a PURCHASESQ. Produkt TORONTO zpřístupňuje tyto fronty ve všech příslušných klastrech, INVENTORY, PAYROLL, SALES a PURCHASES. Definujte seznam názvů klastrů ve správci front produktu TORONTO :

```
DEFINE NAMELIST(TOROLIST)
DESCR('List of clusters TORONTO is in')
NAMES(INVENTORY, PAYROLL, SALES, PURCHASES)
```

Přidejte seznam názvů do každé definice fronty:

```
DEFINE QLOCAL(INVENTQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(PAYROLLQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(SALESQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(PURCHASESQ) CLUSNL(TOROLIST)
```

Nyní předpokládejme, že chcete odebrat všechny tyto fronty z klastru SALES, protože operace SALES má být převzata operací PURCHASES. Vše, co musíte udělat, je změnit seznam názvů produktu TOROLIST a odebrat z něj název klastru SALES.

Chcete-li odebrat jednu frontu z jednoho z klastrů v seznamu názvů, vytvořte seznam názvů obsahující zbývající seznam názvů klastrů. Poté upravte definici fronty tak, aby používala nový seznam názvů. Chcete-li odebrat produkt PAYROLLQ z klastru INVENTORY, postupujte takto:

1. Vytvořte seznam názvů:

```
DEFINE NAMELIST(TOROSHORTLIST)
DESCR('List of clusters TORONTO is in other than INVENTORY')
NAMES(PAYROLL, SALES, PURCHASES)
```

2. Změňte definici fronty produktu PAYROLLQ :

```
ALTER QLOCAL(PAYROLLQ) CLUSNL(TOROSHORTLIST)
```

Odebrání správce front z klastru

Odebírá správce front z klastru v situacích, kdy může správce front normálně komunikovat s alespoň jedním úplným úložištěm v klastru.

Než začnete

Tato metoda je nejlepším postupem pro scénáře, ve kterých je k dispozici alespoň jedno úplné úložiště a může být kontaktováno správcem front, který je odebrán. Tato metoda zahrnuje nejmenší ruční zásah a umožňuje správci front vyjednávat řízené stažení z klastru. Pokud se správce front, který je odstraňován, nemůže spojit s úplným úložištěm, prohlédněte si téma [“Odebrání správce front z klastru: Alternativní metoda”](#) na stránce 287.

Informace o této úloze

Tato vzorová úloha odstraní správce front LONDON z klastru INVENTORY . Klastř INVENTORY je nastaven tak, jak je popsán v části [“Přidání správce front do klastru”](#) na stránce 238, a upraven tak, jak je popsáno v tématu [“Odebrání fronty klastru ze správce front”](#) na stránce 283.

Proces odebrání správce front z klastru je komplikovanější, než je proces přidání správce front.

Když se správce front připojí ke klastru, stávající členové klastru nemají žádné informace o novém správci front, a proto s ním nemají žádné interakce. Je třeba vytvořit nový odesílací a přijímací kanál na připojovaném správci front, aby se mohl připojit k úplnému úložišti.

Je-li správce front odebrán z klastru, je pravděpodobné, že aplikace připojené ke správci front používají objekty, jako jsou fronty, které jsou hostovány jinde v klastru. Aplikace, které jsou připojeny k dalším správcům front v klastru, mohou také používat objekty hostované na cílovém správci front. V důsledku těchto aplikací může aktuální správce front vytvořit další odesílací kanály pro navázání komunikace s jinými členy klastru, než je úplné úložiště, které se používá ke spojení s klastrem. Každý správce front v klastru má kopii dat uloženou v mezipaměti, která popisuje ostatní členy klastru. To může zahrnovat odebrání právě odebírané.

Postup

1. Před odebráním správce front z klastru se ujistěte, že správce front již není hostitelem prostředků potřebných pro klastř:
 - Pokud správce front je hostitelem úplného úložiště, proveďte kroky 1-6 z produktu [“Přesunutí úplného úložiště do jiného správce front”](#) na stránce 249. Pokud funkce úplného úložiště správce front, která má být odebrána, nebude přesunuta do jiného správce front, je třeba provést pouze kroky 5 a 6.
 - Pokud správce front hostí fronty klastru, proveďte kroky 1 až 7 z produktu [“Odebrání fronty klastru ze správce front”](#) na stránce 283.
 - Pokud správce front hostuje témata klastru, buď odstraňte témata (například pomocí příkazu `DELETE TOPIC`), nebo je přesuňte do jiných hostitelů, jak je popsáno v tématu [“Přesun definice tématu klastru do jiného správce front”](#) na stránce 336.

Poznámka: Pokud odeberete správce front z klastru a správce front stále bude hostitelem tématu klastru, může se správce front nadále pokoušet o doručení publikací do správců front, kteří zůstanou v klastru, dokud nebude téma odstraněno.

2. Upravte ručně definované kanály příjemce klastru tak, aby byly odebrány z klastru, ve správci front LONDON:

```
ALTER CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) CLUSTER(' ')
```

3. Upravte ručně definované odesílací kanály klastru tak, aby byly odebrány z klastru, ve správci front LONDON:

```
ALTER CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSSDR) CLUSTER(' ')
```

Ostatní správci front v klastru zjistí, že tento správce front a jeho prostředky klastru již nejsou součástí klastru.

4. Monitorujte přenosovou frontu klastru ve správci front LONDON, dokud zde nebudou žádné zprávy, které čekají na tok do libovolného úplného úložiště v klastru.

```
DISPLAY CHSTATUS(INVENTORY.LONDON) XQMSGSA
```

Pokud zprávy zůstávají ve frontě vysílání, určete, proč nejsou odeslány do úplných úložišť serveru PARIS a NEWYORK, než budete pokračovat.

Výsledky

Správce front LONDON již není součástí klastru. Funkce však může stále fungovat jako nezávislý správce front.

Jak pokračovat dále

Výsledek těchto změn může být potvrzen zadáním následujícího příkazu na zbývající členy klastru:

```
DISPLAY CLUSQMGR(LONDON)
```

Správce front bude nadále zobrazován až do zastavení automaticky definovaného odesílacího kanálu klastru. Můžete počkat, až se to stane, nebo můžete pokračovat v monitorování aktivních instancí zadáním následujícího příkazu:

```
DISPLAY CHANNEL(INVENTORY.LONDON)
```

Pokud jste si jisti, že do tohoto správce front nejsou doručovány žádné další zprávy, můžete odesílací kanály klastru zastavit na serveru LONDON zadáním následujícího příkazu na zbývající členy klastru:

```
STOP CHANNEL(INVENTORY.LONDON) STATUS(INACTIVE)
```

Po šíření změn v celém klastru a do tohoto správce front nebudou doručovány žádné další zprávy, zastavte a odstraňte kanál CLUSRCVR v systému LONDON:

```
STOP CHANNEL(INVENTORY.LONDON)  
DELETE CHANNEL(INVENTORY.LONDON)
```

Odebraného správce front lze do klastru přidat později, jak je popsáno v tématu [“Přidání správce front do klastru”](#) na stránce 238. Odebraný správce front bude nadále ukládat do mezipaměti informace o zbývajících členech klastru po dobu až 90 dnů. Pokud nechcete čekat, dokud tato mezipaměť nevyprší,

může být vynuceně odebrána, jak je popsáno v tématu [“Obnova správce front do stavu před klastrem”](#) na stránce 289.

Odebrání správce front z klastru: Alternativní metoda

Odeberte správce front z klastru, ve scénářích, kde kvůli významnému problému systému nebo konfigurace nemůže správce front komunikovat s žádným úplným úložištěm v klastru.

Než začnete

Tato alternativní metoda odebrání správce front z klastru ručně zastaví a odstraní všechny kanály klastru propojující odebraného správce front s klastrem a vynutí odebrání správce front z klastru. Tato metoda se používá ve scénářích, kdy odebírané správce front nemůže komunikovat s žádným z úplných úložišť. To může být (například), protože správce front přestal pracovat, nebo protože došlo k delšímu komunikačnímu selhání mezi správcem front a klastrem. V opačném případě použijte nejběžnější metodu: [“Odebrání správce front z klastru”](#) na stránce 285.

Informace o této úloze

Tato vzorová úloha odstraní správce front LONDON z klastru INVENTORY . Klastř INVENTORY je nastaven tak, jak je popsán v části [“Přidání správce front do klastru”](#) na stránce 238, a upraven tak, jak je popsáno v tématu [“Odebrání fronty klastru ze správce front”](#) na stránce 283.

Proces odebrání správce front z klastru je komplikovanější, než je proces přidání správce front.

Když se správce front připojí ke klastru, stávající členové klastru nemají žádné informace o novém správci front, a proto s ním nemají žádné interakce. Je třeba vytvořit nový odesílací a přijímací kanál na připojovaném správci front, aby se mohl připojit k úplnému úložišti.

Je-li správce front odebrán z klastru, je pravděpodobné, že aplikace připojené ke správci front používají objekty, jako jsou fronty, které jsou hostovány jinde v klastru. Aplikace, které jsou připojeny k dalším správcům front v klastru, mohou také používat objekty hostované na cílovém správci front. V důsledku těchto aplikací může aktuální správce front vytvořit další odesílací kanály pro navázání komunikace s jinými členy klastru, než je úplné úložiště, které se používá ke spojení s klastrem. Každý správce front v klastru má kopii dat uloženou v mezipaměti, která popisuje ostatní členy klastru. To může zahrnovat odebrání právě odebírané.

Tento postup může být v případě nouze vhodný, nelze-li čekat na to, aby správce front opustil klastř hladce.

Postup

1. Před odebráním správce front z klastru se ujistěte, že správce front již není hostitelem prostředků potřebných pro klastř:
 - Pokud správce front je hostitelem úplného úložiště, proveďte kroky 1-6 z produktu [“Přesunutí úplného úložiště do jiného správce front”](#) na stránce 249. Pokud funkce úplného úložiště správce front, která má být odebrána, nebude přesunuta do jiného správce front, je třeba provést pouze kroky 5 a 6.
 - Pokud správce front hostí fronty klastru, proveďte kroky 1 až 7 z produktu [“Odebrání fronty klastru ze správce front”](#) na stránce 283.
 - Pokud správce front hostuje témata klastru, buď odstraňte témata (například pomocí příkazu `DELETE TOPIC`), nebo je přesuňte do jiných hostitelů, jak je popsáno v tématu [“Přesun definice tématu klastru do jiného správce front”](#) na stránce 336.

Poznámka: Pokud odeberete správce front z klastru a správce front stále bude hostitelem tématu klastru, může se správce front nadále pokoušet o doručení publikací do správců front, kteří zůstanou v klastru, dokud nebude téma odstraněno.
2. Zastavte všechny kanály používané ke komunikaci s ostatními správci front v klastru. Pomocí příkazu `MODE (FORCE)` lze kanál `CLUSRCVR` zastavit ve správci front `LONDON`. V opačném případě může být třeba počkat, až správce front odesílatele zastaví kanál:

```
STOP CHANNEL(INVENTORY.LONDON) MODE(FORCE)
STOP CHANNEL(INVENTORY.TORONTO)
STOP CHANNEL(INVENTORY.PARIS)
STOP CHANNEL(INVENTORY.NEWYORK)
```

3. Sledujte stavy kanálů ve správci front LONDON až do zastavení kanálů:

```
DISPLAY CHSTATUS(INVENTORY.LONDON)
DISPLAY CHSTATUS(INVENTORY.TORONTO)
DISPLAY CHSTATUS(INVENTORY.PARIS)
DISPLAY CHSTATUS(INVENTORY.NEWYORK)
```

Po zastavení kanálů se do ostatních správců front v klastru neodesílají žádné další zprávy aplikací.

4. Odstraňte ručně definované kanály klastru ve správci front LONDON:

```
DELETE CHANNEL(INVENTORY.NEWYORK)
DELETE CHANNEL(INVENTORY.TORONTO)
```

5. Zbývající správci front v klastru si stále uchovávají znalosti odebraného správce front a mohou k němu i nadále odesílat zprávy. Chcete-li vymazat znalosti ze zbývajících správců front, resetujte odebraného správce front z klastru na jednom z úplných úložišť:

```
RESET CLUSTER(INVENTORY) ACTION(FORCEREMOVE) QMNAME(LONDON) QUEUES(YES)
```

Může-li existovat jiný správce front v klastru, který má stejný název jako odebraný správce front, zadejte **QMID** odebraného správce front.

Výsledky

Správce front LONDON již není součástí klastru. Funkce však může stále fungovat jako nezávislý správce front.

Jak pokračovat dále

Výsledek těchto změn může být potvrzen zadáním následujícího příkazu na zbývajících členech klastru:

```
DISPLAY CLUSQMGR(LONDON)
```

Správce front bude nadále zobrazován až do zastavení automaticky definovaného odesílacího kanálu klastru. Můžete počkat, až se to stane, nebo můžete pokračovat v monitorování aktivních instancí zadáním následujícího příkazu:

```
DISPLAY CHANNEL(INVENTORY.LONDON)
```

Po šíření změn v celém klastru a do tohoto správce front nejsou doručovány žádné další zprávy, odstraňte kanál produktu CLUSRCVR v systému LONDON:

```
DELETE CHANNEL(INVENTORY.LONDON)
```

Odebraného správce front lze do klastru přidat později, jak je popsáno v tématu [“Přidání správce front do klastru”](#) na stránce 238. Odebraný správce front bude nadále ukládat do mezipaměti informace o zbývajících členech klastru po dobu až 90 dnů. Pokud nechcete čekat, dokud tato mezipaměť nevyprší, může být vynuceně odebrána, jak je popsáno v tématu [“Obnova správce front do stavu před klastrem”](#) na stránce 289.

Obnova správce front do stavu před klastrem

Je-li správce front odebrán z klastru, uchovává informace o zbývajících členech klastru. Tyto znalosti nakonec vyprší a budou odstraněny automaticky. Pokud však chcete tuto akci odstranit okamžitě, můžete použít kroky uvedené v tomto tématu.

Než začnete

Předpokládá se, že správce front byl odebrán z klastru a že již neprovádí žádnou práci v klastru. Například, její fronty již nepřijímají zprávy z klastru a žádné aplikace nečekají na doručení zpráv do těchto front.

Informace o této úloze

Je-li správce front odebrán z klastru, uchovává znalosti o zbývajících členech klastru po dobu až 90 dnů. Může mít systémové výhody, zvláště pokud se správce front rychle znovu připojí ke klastru. Po konečném vypršení platnosti této znalosti dojde k automatickému odstranění tohoto souboru. Existují však důvody, proč byste měli raději tyto informace odstranit ručně. Příklad:

- Možná budete chtít potvrdit, že jste zastavili každou aplikaci v tomto správcí front, která dříve používala prostředky klastru. Dokud nedojde k vypršení platnosti znalostí zbývajících členů klastru, bude každá taková aplikace pokračovat v zápisu do přenosové fronty. Po odstranění znalostí klastru systém vygeneruje chybovou zprávu, když se taková aplikace pokusí použít prostředky klastru.
- Zobrazíte-li informace o stavu správce front, můžete raději nezobrazovat informace o skončení platnosti zbývajících členů klastru.

Tato úloha používá klastr INVENTORY jako příklad. Správce front produktu LONDON byl odebrán z klastru INVENTORY, jak je popsáno v tématu [“Odebrání správce front z klastru”](#) na stránce 285. Chcete-li odstranit informace o zbývajících členech klastru, zadejte ve správcí front produktu LONDON následující příkazy.

Postup

1. Odeberte veškerou paměť ostatních správců front v klastru z tohoto správce front:

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

2. Monitorujte správce front, dokud nebudou všechny prostředky klastru pryč:

```
DISPLAY CLUSQMR(*) CLUSTER(INVENTORY)  
DISPLAY QCLUSTER(*) CLUSTER(INVENTORY)  
DISPLAY TOPIC(*) CLUSTER(INVENTORY)
```

Související informace

[Klastry](#)

[Porovnání klastrování a distribuovaných front](#)

[Komponenty klastru](#)

Údržba správce front

Chcete-li provést údržbu, pozastavte a obnovte správce front z klastru.

Informace o této úloze

Čas od času může být nutné provést údržbu u správce front, který je součástí klastru. Například můžete potřebovat provést zálohování dat ve svých frontách nebo použít opravy na software. Pokud správce front je hostitelem jakýchkoli front, je třeba jeho aktivity pozastavit. Když je údržba dokončena, její aktivity mohou být obnoveny.

Postup

1. Pozastavit správce front zadáním příkazu SUSPEND QMGR **runmqsc** :

```
SUSPEND QMGR CLUSTER(SALES)
```

Příkaz SUSPEND **runmqsc** oznamuje správci front v klastru SALES , že tento správce front byl pozastaven.

Účelem příkazu SUSPEND QMGR je pouze informovat ostatní správce front, aby se vyhnuli odesílání zpráv do tohoto správce front, je-li to možné. Neznamená to, že správce front je zakázán. Některé zprávy, které mají být zpracovány tímto správcem front, jsou stále k sobě odeslány, například když je tento správce front jediným hostitelem klastrované fronty.

Když je správce front pozastaven, rutiny správy pracovní zátěže se vyhnou odesílání zpráv do tohoto modulu. Zprávy, které mají být zpracovány tímto správcem front, zahrnují zprávy odeslané lokálním správcem front.

IBM MQ používá algoritmus vyrovnávání pracovní zátěže k určení toho, která místa určení jsou vhodná, místo toho, aby bylo možné kdykoli vybrat lokálního správce front.

- a) Vynucení pozastavení správce front pomocí volby FORCE v příkazu SUSPEND QMGR :

```
SUSPEND QMGR CLUSTER(SALES) MODE(FORCE)
```

Produkt MODE (FORCE) vynutí zastavení všech přichozích kanálů od jiných správců front v klastru. Pokud ne zadáte MODE (FORCE) , použije se výchozí MODE (QUIESCE) .

2. Proveďte všechny úlohy údržby potřebné.
3. Obnovte správce front zadáním příkazu RESUME QMGR **runmqsc** :

```
RESUME QMGR CLUSTER(SALES)
```

Výsledky


Příkaz RESUME **runmqsc** upozorňuje na úplná úložiště, která je správce front k dispozici znovu. Správci front úplného úložiště šíří tyto informace do jiných správců front, kteří požádali o aktualizace informací o tomto správcem front.

Údržba přenosové fronty klastru

Učinit veškeré úsilí, aby byly k dispozici přenosové fronty klastru. Jsou nezbytné pro výkon klastrů.

 V z/OS nastavte INDXTYPE přenosové fronty klastru na CORRELID.

Než začnete

- Ujistěte se, že se přenosová fronta klastru nezaplňuje.
- Dávejte pozor, abyste nevydali příkaz ALTER **runmqsc** k nastavení, ať se deaktivuje nebo deaktivuje omylem.
- Ujistěte se, že médium přenosové fronty klastru je uloženo v  (například z/OS sad stránek) , nebude zaplněno.

Informace o této úloze



Následující procedura se vztahuje pouze na z/OS.

Postup

Nastavte INDXTYPE přenosové fronty klastru na CORRELID

Obnova správce front klastru

Pomocí příkazu REFRESH CLUSTER lze odebrat automaticky definované kanály a automaticky definované objekty klastru z lokálního úložiště. Žádné zprávy nejsou ztraceny.

Než začnete

Můžete být požádáni o použití příkazu pro centrum podpory produktu IBM . Nepoužívejte tento příkaz bez důkladného uvážení. Například u velkých klastrů pomocí příkazu **REFRESH CLUSTER** může dojít k přerušení činnosti klastru při jeho průběhu, a poté znovu ve 27. denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zúčastněným správcům front. Viz [Klastrování: Použití doporučených postupů REFRESH CLUSTER](#).

Informace o této úloze

Správce front může vytvořit nový začátek v klastru. Za normálních okolností není třeba použít příkaz REFRESH CLUSTER .

Postup

Zadáním příkazu REFRESH CLUSTER **MQSC** ze správce front odeberte automaticky definované objekty správce front klastru a fronty z lokálního úložiště.

Tento příkaz pouze odebere objekty, které odkazují na jiné správce front, neodebere objekty související s lokálním správcem front. Příkaz také odebere automaticky definované kanály. Odebírá kanály, které nemají zprávy v přenosové frontě klastru a nejsou připojeny k úplnému správci front úložiště.

Výsledky

Ve skutečnosti příkaz REFRESH CLUSTER umožňuje, aby správce front byl studený s ohledem na obsah celého úložiště. Produkt IBM MQ zajišťuje, že ve frontách nebudou ztracena žádná data.

Související informace

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

Obnova správce front klastru

Pomocí příkazu REFRESH CLUSTER **runmqsc** převedte informace o klastru do aktuálního správce front až do data. Postupujte podle této procedury po obnovení správce front z bodu v časovém okamžiku.

Než začnete

Obnovili jste správce front klastru ze zálohy k určitému časovému bodu.

Informace o této úloze

Chcete-li obnovit správce front v klastru, obnovte správce front a poté uveďte informace o klastru do data pomocí příkazu REFRESH CLUSTER **runmqsc** .

Poznámka: U velkých klastrů může být použit příkaz **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](#).

Postup

Zadejte příkaz REFRESH CLUSTER v obnoveném správci front pro všechny klastry, jichž se správce front účastní.

Jak pokračovat dále

V žádném jiném správci front není třeba zadávat příkaz REFRESH CLUSTER .

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Konfigurace kanálů klastru pro dostupnost

Postupujte podle správných postupů konfigurace, aby kanály klastru běžela bez problémů, pokud existují přerušované zastavování sítě.

Než začnete

Klastry vás zbavují nutnosti definovat kanály, ale přesto je musíte udržovat. Stejná technologie kanálu se používá pro komunikaci mezi správci front v klastru tak, jak se používá v distribuovaných frontách. Chcete-li porozumět kanálům klastru, musíte být obeznámeni s otázkami, jako jsou například:

- Způsob fungování kanálů
- Jak zjistit jejich stav
- Jak používat uživatelské procedury kanálu

Informace o této úloze

Možná byste měli věnovat zvláštní pozornost následujícím bodům:

Postup

Při konfiguraci kanálů klastru zvažte následující body

- Vyberte hodnoty pro HBINT nebo KAINTE na odesílacích kanálech klastru a přijímacích kanálech klastru, které nezatěžují síť se spoustou synchronizačních signálů nebo s udržováním živých toků. Interval kratší než přibližně 10 sekund dává falešné selhání, pokud se vaše síť někdy zpomaluje a zavádí zpoždění této délky.
- Nastavte hodnotu parametru BATCHHB tak, aby se okno snížilo, protože je to nejisté, protože je to u kanálu, u kterého došlo k selhání. Nejistá dávka na kanálu, u kterého došlo k selhání, se bude pravděpodobně vyskytnout v případě, že je dávka již zaplněna. Je-li provoz zpráv v rámci kanálu sporadický s dlouhými časovými úseky mezi shlukováním zpráv, je pravděpodobnější, že je dávka neúspěšná.
- Problém vzniká tehdy, když se konec kanálu odesílatele klastru nezdaří a poté se pokusí o restartování před tím, než prezenční signál nebo udržení aktivity zjistí selhání. Restart channel-sender je odmítnut, pokud byl konec kanálu klastru, který byl příjemcem aktivní, aktivní. Chcete-li se vyhnout selhání, zařídte, aby se kanál příjemce klastru ukončil a restartoval, když se kanál odesílatele klastru pokusí o restart.

zapIBM MQ for z/OS

Řídí problém konce příjemce klastru, který zůstává aktivní pomocí parametrů ADOPTMCA a ADOPTCHK v systému ALTER QMGR.

Na platformách jiných než z/OS

Řídí problém konce příjemce klastru, který zůstává aktivní pomocí atributů AdoptNewMCA, AdoptNewMCATimeout a AdoptNewMCACheck v souboru qm.ini nebo v registru Windows NT .

Směrování zpráv do a z klastrů

Alias fronty, aliasy správců front a definice vzdálených front slouží k připojení klastrů k externím správcům front a dalším klastrům.

Podrobnosti o směrování zpráv do a z klastrů naleznete v následujících dílčích tématech:

Související pojmy

[“Alias správce front a klastry” na stránce 306](#)

Alias správce front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

[“Alias fronty a klastry” na stránce 309](#)

Alias fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

[“Alias fronty pro odpověď a klastry” na stránce 308](#)

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Související úlohy

[“Konfigurace klastru správce front” na stránce 216](#)

Klastry poskytují mechanismus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

[“Nastavení nového klastru” na stránce 228](#)

Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

Související informace

[Klastry](#)

[Porovnání klastrování a distribuovaných front](#)

[Komponenty klastru](#)

Konfigurace požadavku/odpovědi na klastr

Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

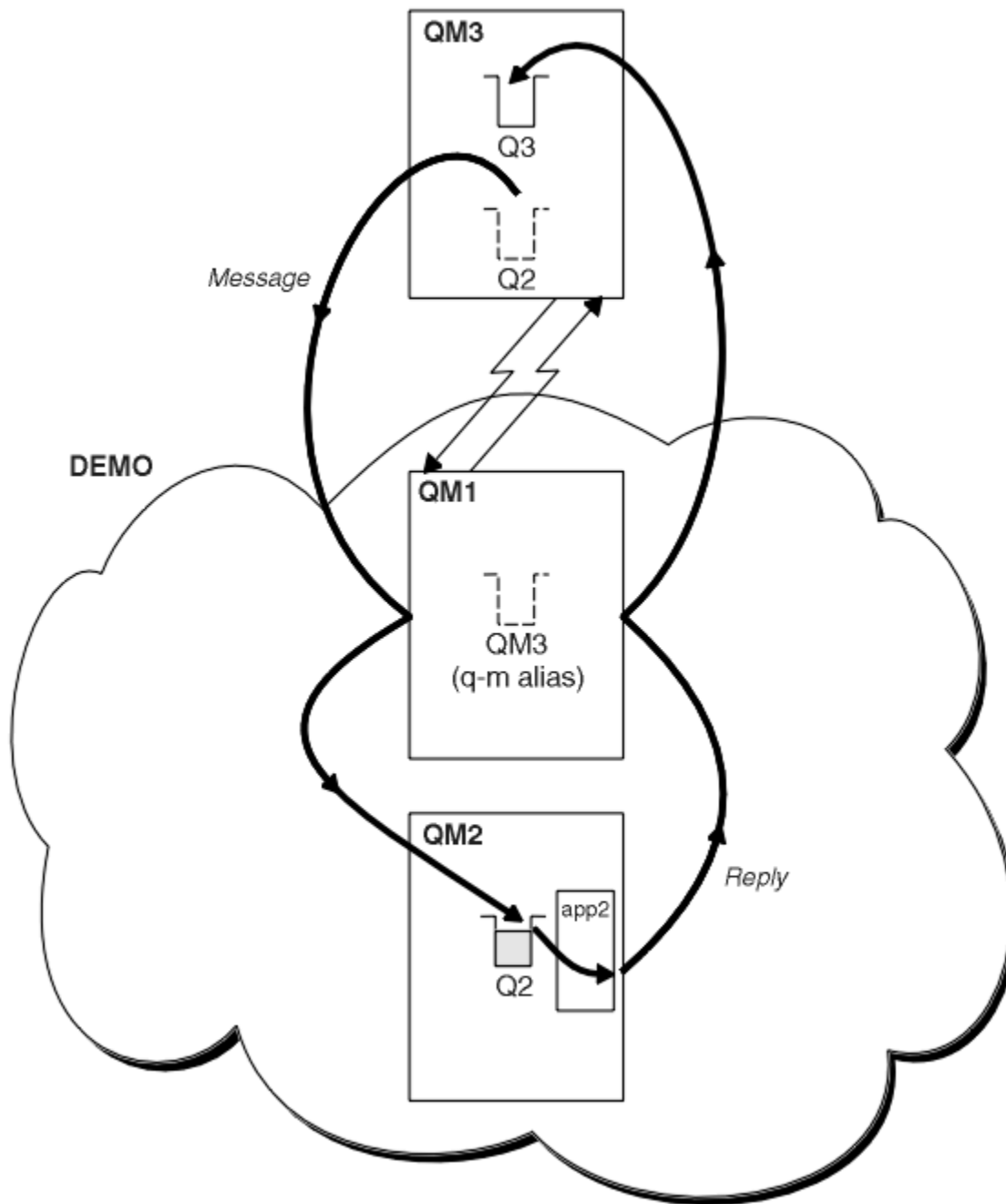
Než začnete

Produkt Obrázek 54 na stránce 294 zobrazuje správce front s názvem QM3, který se nachází mimo klastr s názvem DEMO. QM3 může být správce front na produktu IBM MQ, který nepodporuje klastry. QM3 je hostitelem fronty s názvem Q3, která je definována takto:

```
DEFINE QLOCAL(Q3)
```

Uvnitř klastru jsou dva správci front s názvem QM1 a QM2. Produkt QM2 je hostitelem fronty klastru s názvem Q2, která je definována takto:

```
DEFINE QLOCAL(Q2) CLUSTER(DEMO)
```



Obrázek 54. Vložení ze správce front mimo klastr

Informace o této úloze

Chcete-li nastavit cestu pro zprávy požadavku a odpovědi, postupujte podle pokynů v proceduře.

Postup

1. Odešlete zprávu požadavku do klastru.

Zvažte, jakým způsobem správce front, který je mimo klastr, vloží zprávu do fronty Q2 na QM2, která je uvnitř klastru. Správce front mimo klastr musí mít definici QREMOTE pro každou frontu v klastru, do které umísťuje zprávy.

- a) Definujte vzdálenou frontu pro Q2 v systému QM3.

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(QM2) XMITQ(QM1)
```

Protože produkt QM3 není součástí klastru, musí komunikovat s použitím distribuovaných technik řazení do fronty. Proto musí mít také odesílací kanál a přenosovou frontu na QM1. Produkt QM1 potřebuje odpovídající přijímací kanál. Kanály a přenosové fronty nejsou explicitně zobrazeny v produktu [Obrázek 54 na stránce 294](#).

V tomto příkladu aplikace v produktu QM3 vydá výzvu MQPUT k vložení zprávy do produktu Q2. Definice QREMOTE způsobí, že se zpráva bude směřována do Q2 v QM2 pomocí odesílacího kanálu, který získává zprávy z přenosové fronty QM1 .

2. Přijmout zprávu odpovědi z klastru.

Alias správce front slouží k vytvoření návratové cesty pro odpovědi na správce front mimo klastr. Brána, QM1, inzeruje alias správce front pro správce front mimo klastr QM3. Potvrdí produkt QM3 správcům front v rámci klastru přidáním atributu klastru do definice aliasu správce front produktu QM3. Definice aliasu správce front je jako definice vzdálené fronty, ale s prázdnou hodnotou RNAME.

a) Definujte alias správce front pro produkt QM3 v systému QM1.

```
DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
```

Musíme zvážit volbu názvu přenosové fronty použité k předání odpovědi zpět z produktu QM1 do produktu QM3. Implicitně v definici QREMOTE je při vynechání atributu XMITQ název přenosové fronty QM3. Ale QM3 je stejný název, jaký očekáváme, že inzerovat na zbytek klastru pomocí aliasu správce front. Produkt IBM MQ neumožňuje zadat název přenosové fronty i alias správce front se stejným názvem. Jedním z řešení je vytvoření přenosové fronty pro předávání zpráv do produktu QM3 s jiným názvem než alias správce front.

b) Zadejte název přenosové fronty do definice QREMOTE .

```
DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO) XMITQ(QM3.XMIT)
```

Alias nového správce front spojuje novou přenosovou frontu s názvem QM3 . XMIT s aliasem správce front QM3 . Je to jednoduché a správné řešení, ale ne zcela uspokojivé. Porušeno konvence pojmenování pro přenosové fronty, které mají stejný název jako cílový správce front. Existují nějaká alternativní řešení, která zachovávají konvence pojmenování přenosových front?

Problém vzniká, protože žadatel standardně předává QM3 jako název správce front odpovědi ve zprávě s požadavkem, který je odeslán z produktu QM3. Server v produktu QM2 používá název správce front pro odpověď QM3 na adresu QM3 ve svých odpovědích. Řešení požaduje produkt QM1 k inzerování produktu QM3 jako alias správce front, aby vrátil zprávy s odpovědí a zabránil produktu QM1 v používání produktu QM3 jako názvu přenosové fronty.

Místo toho, aby jako výchozí název správce front byl zadán QM3 jako název správce front odpovědi, musí aplikace v produktu QM3 předat alias odpovědi správce front produktu QM1 pro zprávy odpovědí. Správce front brány QM1 inzeruje alias správce front pro odpovědi na QM3 spíše než o samotnou QM3 a vyhýbá se konfliktu s názvem přenosové fronty.

c) Definujte alias správce front pro produkt QM3 v systému QM1.

```
DEFINE QREMOTE(QM3.ALIAS) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
```

Jsou vyžadovány dvě změny konfiguračních příkazů.

i) Produkt QREMOTE v QM1 nyní oznamuje svůj alias správce front QM3 . ALIAS zbytku klastru a pojmenuje jej na název skutečného správce front QM3. QM3 je znovu název přenosové fronty, která má odeslat fronty odpovědi zpět na QM3

ii) Klientská aplikace musí poskytovat QM3 . ALIAS jako název správce front pro odpovědi, když vytváří zprávu požadavku. QM3 . ALIAS klientské aplikaci můžete poskytnout dvěma způsoby aplikaci klienta.

- Kód QM3 . ALIAS je v poli názvu správce front pro odpověď sestaveno pomocí MQPUT v MQMD. Musíte to provést tímto způsobem, pokud používáte dynamickou frontu pro odpovědi.
- Při zadávání názvu fronty pro odpověď použijte alias fronty k odpovědi, Q3 . ALIAS, spíše než frontu pro odpověď.

```
DEFINE QREMOTE(Q3.ALIAS) RNAME(Q3) RQMNAME(QM3.ALIAS)
```

Jak pokračovat dále

Poznámka: Nemůžete demonstrovat použití aliasů fronty odpovědi s **AMQSREQ0**. Otevře frontu pro odpověď s použitím názvu fronty uvedeného v parametru 3 nebo ve výchozí modelové frontě produktu SYSTEM . SAMPLE . REPLY . Musíte upravit ukázkou poskytující jiný parametr obsahující alias fronty pro odpověď pro pojmenování alias správce front pro produkt MQPUT pro odpověď.

Související pojmy

Alias správce front a klastry

Alias správce front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Alias fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Alias fronty a klastry

Alias fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry

Spojte klastry společně s použitím správce front brány. Učinit fronty nebo správce front viditelné pro všechny klastry definováním aliasů fronty klastru nebo správce front klastru ve správci front brány.

“Skrytí názvu cílového správce front klastru” na stránce 296

Zasměřujte zprávu do fronty klastru, která je definovaná na libovolném správci front v klastru, aniž byste pojmenovali správce front.

Skrytí názvu cílového správce front klastru

Zasměřujte zprávu do fronty klastru, která je definovaná na libovolném správci front v klastru, aniž byste pojmenovali správce front.

Než začnete

- Vyhněte se odhalení názvů správců front, kteří jsou v klastru, ke správcům front, kteří nejsou členy klastru.
 - Vyřešení odkazů na správce front, který je hostitelem fronty v klastru, odebere flexibilitu při vyrovnávání pracovní zátěže.
 - Také je pro vás obtížné změnit správce front, který je hostitelem fronty v klastru.

- Alternativou je nahradit parametr RQMNAME aliasem správce front poskytnutým administrátorem klastru.
- Produkt “[Skrytí názvu cílového správce front klastru](#)” na stránce 296 popisuje použití aliasu správce front k odpojení správce front mimo klastr ze správy správců front v rámci klastru.
- Navrhovaným způsobem, jak pojmenovat přenosové fronty, je však poskytnout jim název cílového správce front. Název přenosové fronty odhaluje název správce front v klastru. Musíte zvolit, které pravidlo chcete sledovat. Název přenosové fronty můžete pojmenovat buď pomocí názvu správce front, nebo pomocí názvu klastru:

Pojmenujte přenosovou frontu s použitím názvu správce front brány

Zveřejňování názvu správce front brány pro správce front mimo klastr je vhodnou výjimkou pravidla skrývání názvů správců front klastru.

Pojmenujte přenosovou frontu s použitím názvu klastru.

Pokud se nekonvencí pojmenování přenosových front pojmenováváte pomocí názvu cílového správce front, použijte název klastru.

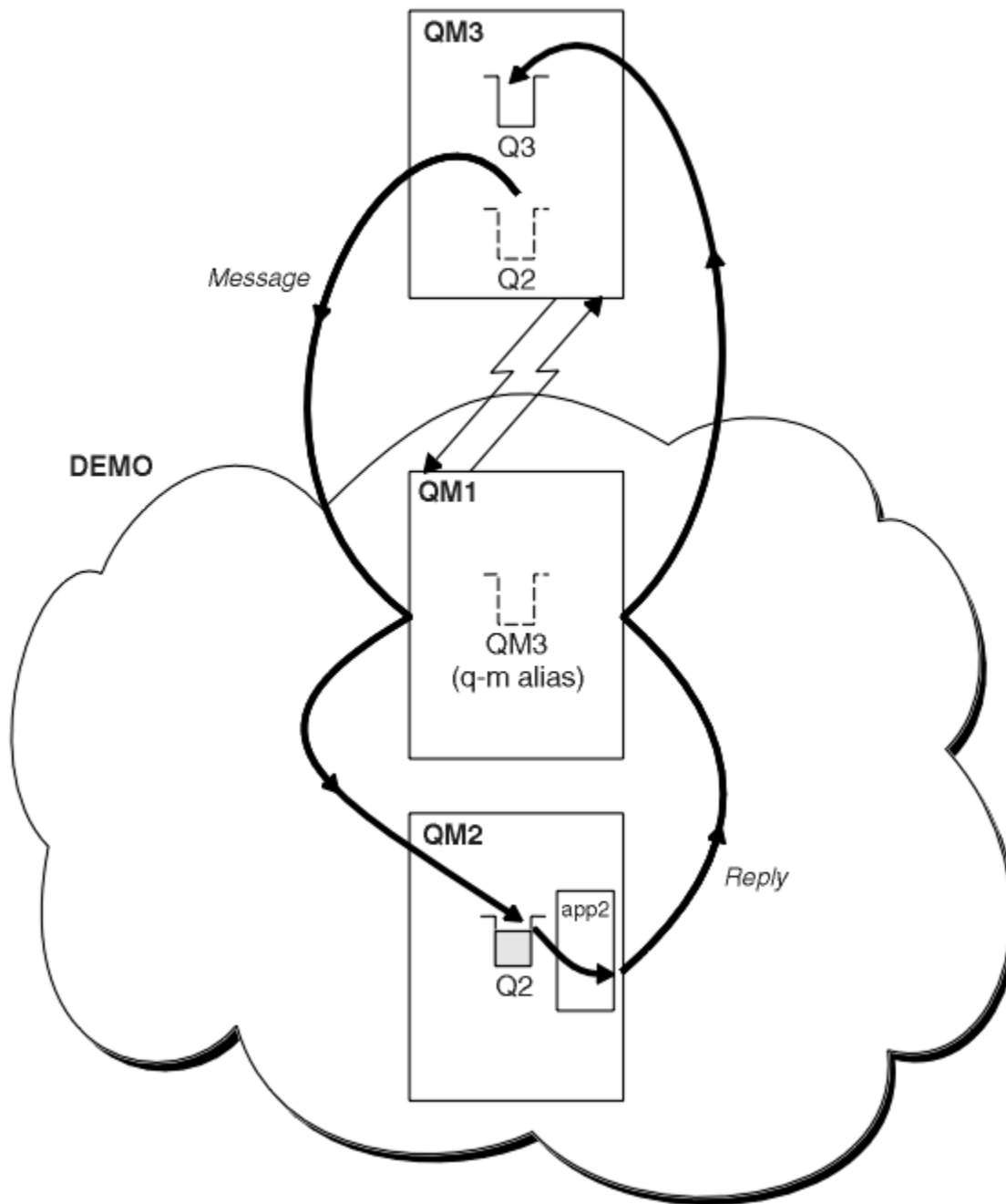
Informace o této úloze

Upravte úlohu “[Konfigurace požadavku/odpovědi na klastr](#)” na stránce 293 tak, abyste skryli název cílového správce front v rámci klastru.

Postup

V tomto příkladu si prohlédněte téma [Obrázek 55 na stránce 298](#), definujte alias správce front ve správci front brány QM1 s názvem DEMO:

```
DEFINE QREMOTE(DEMO) RNAME(' ') RQMNAME(' ')
```



Obrázek 55. Vložení ze správce front mimo klastr

Definice QREMOTE v systému QM1 způsobí, že správce front DEMO alias správce front je znám jako správce front brány. QM3, správce front mimo klastr může pomocí aliasu správce front DEMO odesílat zprávy do klastrovaných front v produktu DEMO místo toho, aby bylo nutné použít skutečné jméno správce front.

Pokud převzmu konvenci použití názvu klastru k pojmenování přenosové fronty připojující se ke klastru, stane se definice vzdálené fronty pro produkt Q2 :

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(DEMO) XMIT(DEMO)
```

Výsledky

Zprávy určené pro Q2 v umístění DEMO jsou umístěny do přenosové fronty DEMO . Z přenosové fronty jsou přenášeny odesílacím kanálem do správce front brány, QM1. Správce front brány směřuje zprávy do libovolného správce front v klastru, který je hostitelem fronty klastru Q2.

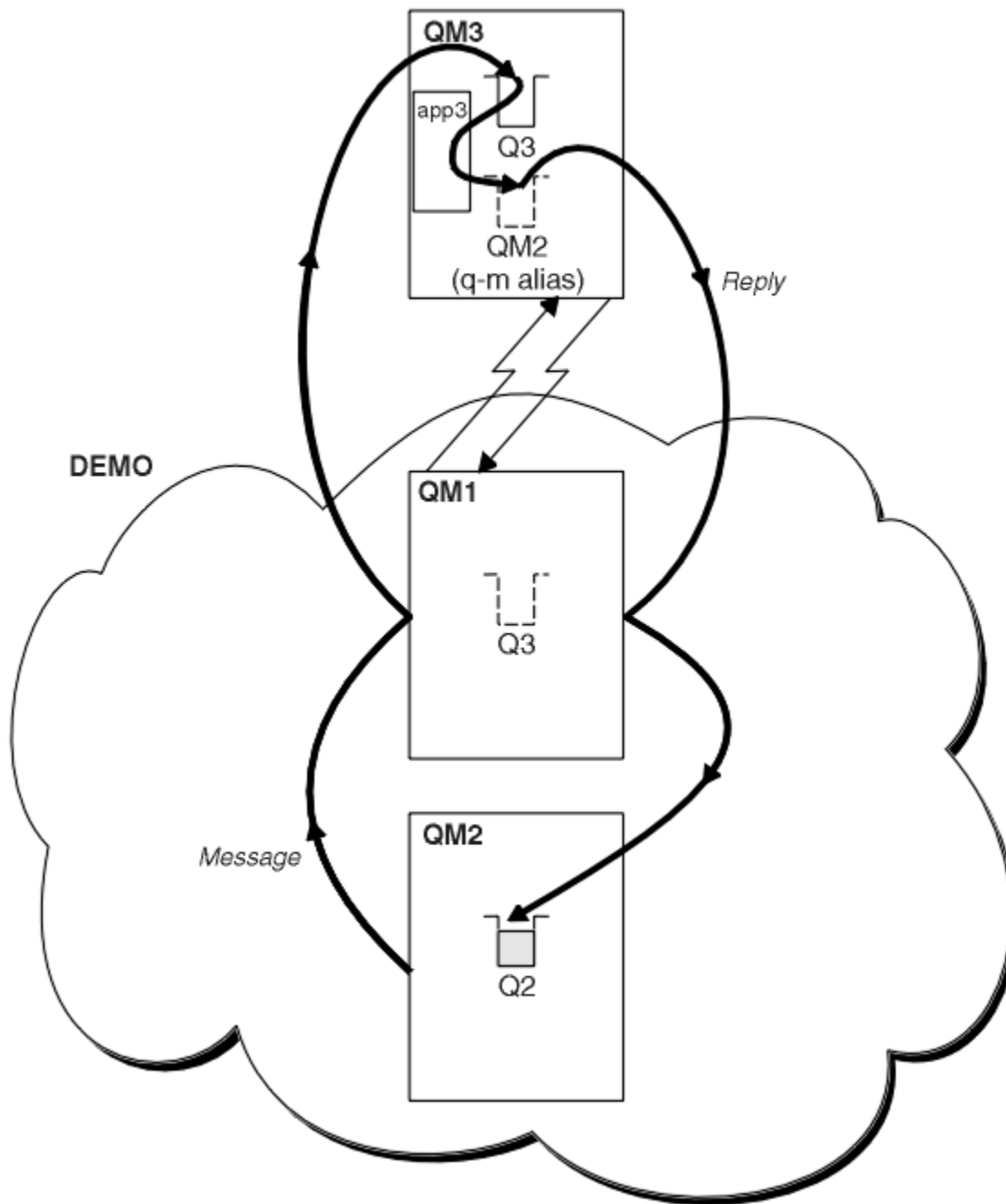
Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Než začnete

Obrázek 56 na stránce 300 zobrazuje správce front QM2, uvnitř klastru DEMO. Odešle požadavek do fronty Q3, jehož hostitelem je správce front mimo klastr. Odpovědi jsou vráceny produktu Q2 v umístění QM2 v klastru.

Chcete-li komunikovat se správcem front mimo klastr, jeden nebo více správců front v rámci klastru se chová jako brána. Správce front brány má komunikační cestu ke správcům front mimo klastr. V tomto příkladu je QM1 brána.



Obrázek 56. Uvedení do správce front mimo klastr

Informace o této úloze

Postupujte podle pokynů pro nastavení cesty pro zprávy požadavku a odpovědi

Postup

1. Odešlete zprávu požadavku z klastru.

Zvažte, jakým způsobem správce front QM2, který je uvnitř klastru, vloží zprávu do fronty Q3 v QM3, která je mimo klastr.

- a) Vytvořte definici QREMOTE na QM1, která označuje vzdálenou frontu Q3 do klastru.

```
DEFINE QREMOTE(Q3) RNAME(Q3) RQMNAME(QM3) CLUSTER(DEMO)
```

Má také odesílací kanál a přenosovou frontu ke správci front, který je mimo klastr. QM3 má odpovídající přijímací kanál. Kanály nejsou zobrazeny v [Obrázek 56 na stránce 300](#).

Aplikace v systému QM2 vydává volání MQPUT určující cílovou frontu a frontu, do níž mají být odesílány odpovědi. Cílová fronta je Q3 a fronta odpovědi je Q2.

Zpráva se odešle na server QM1, který používá svou definici vzdálené fronty k vyřešení názvu fronty do produktu Q3 v QM3.

2. Přijmout zprávu odpovědi od správce front mimo klastr.

Správce front mimo klastr musí mít alias správce front pro každého správce front v klastru, do kterého má odeslat zprávu. Alias správce front musí také určovat název přenosové fronty ke správci front brány. V tomto příkladu produkt QM3 potřebuje definici aliasu správce front pro produkt QM2:

a) Vytvořit alias správce front QM2 v systému QM3

```
DEFINE QREMOTE(QM2) RNAME(' ') RQMNAME(QM2) XMITQ(QM1)
```

Produkt QM3 také potřebuje odesílací kanál a přenosovou frontu pro QM1 a QM1 potřebuje odpovídající přijímací kanál.

Aplikace, **app3**, na QM3 může potom odesílat odpovědi na QM2, zadáním volání MQPUT a zadáním názvu fronty, Q2 a názvu správce front QM2.

Jak pokračovat dále

Můžete definovat více než jednu trasu z klastru.

Související pojmy

Alias správce front a klastry

Alias správce front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Alias fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Alias fronty a klastry

Alias fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr

Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry

Spojte klastry společně s použitím správce front brány. Učinit fronty nebo správce front viditelné pro všechny klastry definováním aliasů fronty klastru nebo správce front klastru ve správci front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Než začnete

Nakonfigurujte příklad, jak je zobrazeno v [Obrázek 54 na stránce 294](#) v “[Konfigurace požadavku/odpovědi na klastr](#)” na stránce 293.

Informace o této úloze

V tomto scénáři správce front mimo klastr, QM3 v [Obrázek 57 na stránce 303](#), odesílá požadavky do fronty Q2. Q2 je hostován na dvou správcích front, QM2 a QM4 v rámci klastru DEMO. Oba správci front jsou konfigurováni s volbou výchozí vazby NOTFIXED, aby bylo možné použít vyrovnávání pracovní zátěže. Požadavky z produktu QM3, správce front mimo klastr, jsou odeslány do instance produktu Q2 prostřednictvím produktu QM1.

QM3 není součástí klastru a komunikuje pomocí technik distribuovaných front. Musí mít odesílací kanál a přenosovou frontu na QM1. Produkt QM1 potřebuje odpovídající přijímací kanál. Kanály a přenosové fronty nejsou explicitně zobrazeny v produktu [Obrázek 57 na stránce 303](#).

Procedura rozšiřuje příklad v produktu [Obrázek 54 na stránce 294](#) v produktu [“Konfigurace požadavku/odpovědi na klastr” na stránce 293](#).

Postup

1. Vytvořte definici QREMOTE pro Q2 na QM3.

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(Q3) XMITQ(QM1)
```

Vytvořte definici QREMOTE pro každou frontu v klastru, do které produkt QM3 vkládá zprávy.

2. Vytvořte alias správce front Q3 v systému QM1.

```
DEFINE QREMOTE(Q3) RNAME(' ') RQMNAME(' ')
```

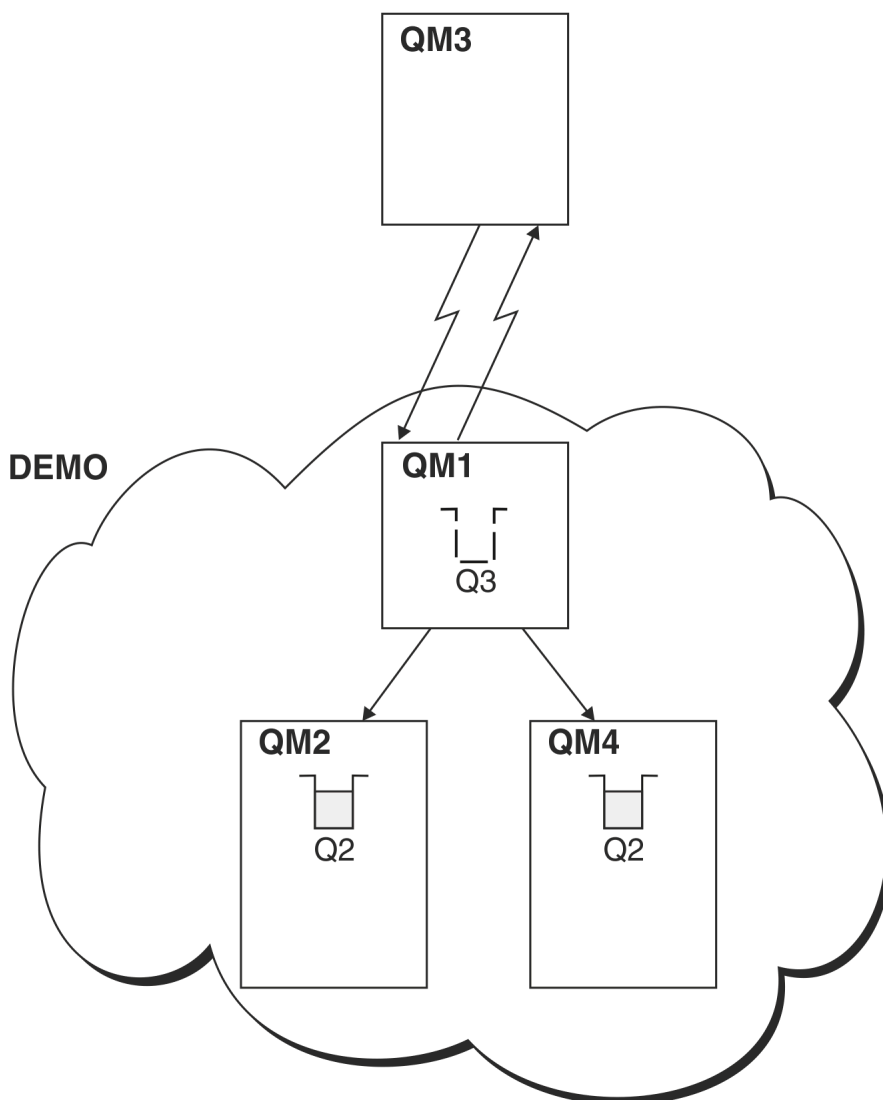
Q3 není název skutečného správce front. Jedná se o název definice aliasu správce front v klastru, který odpovídá názvu aliasu správce front Q3 s prázdnou hodnotou ' '.

3. Definujte lokální frontu s názvem Q2 na každém z QM2 a QM4.

```
DEFINE QLOCAL(Q2) CLUSTER(DEMO) DEFBIND(NOTFIXED)
```

4. QM1, nemá správce front brány žádné speciální definice.

Výsledky



Obrázek 57. Vložení ze správce front mimo klastr

Když aplikace v QM3 vyvolá výzvu MQPUT k vložení zprávy do Q2, definice QREMOTE na QM3 způsobí, že zpráva bude směřována přes správce front brány QM1. Když produkt QM1 přijme zprávu, je si vědom toho, že zpráva je stále zamýšlena pro frontu s názvem Q2 a provádí rozlišení názvu. Produkt QM1 kontroluje lokální definice a nenalezl nic pro Q2. Produkt QM1 poté zkontroluje konfiguraci klastru a zjistí, že je informován o dvou instancích produktu Q2 v klastru DEMO. Produkt QM1 může nyní využívat vyrovňování pracovní zátěže k distribuci zpráv mezi instancemi portálu Q2 umístěnými na QM2 a QM4.

Související pojmy

Aliasy správce front a klastry

Aliasy správce front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Aliasy fronty a klastry

Aliasy fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr

Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace cest zpráv mezi klastry

Spojte klastry společně s použitím správce front brány. Učinit fronty nebo správce front viditelné pro všechny klastry definováním aliasů fronty klastru nebo správce front klastru ve správci front brány.

Související informace

Rozlišení názvu fronty

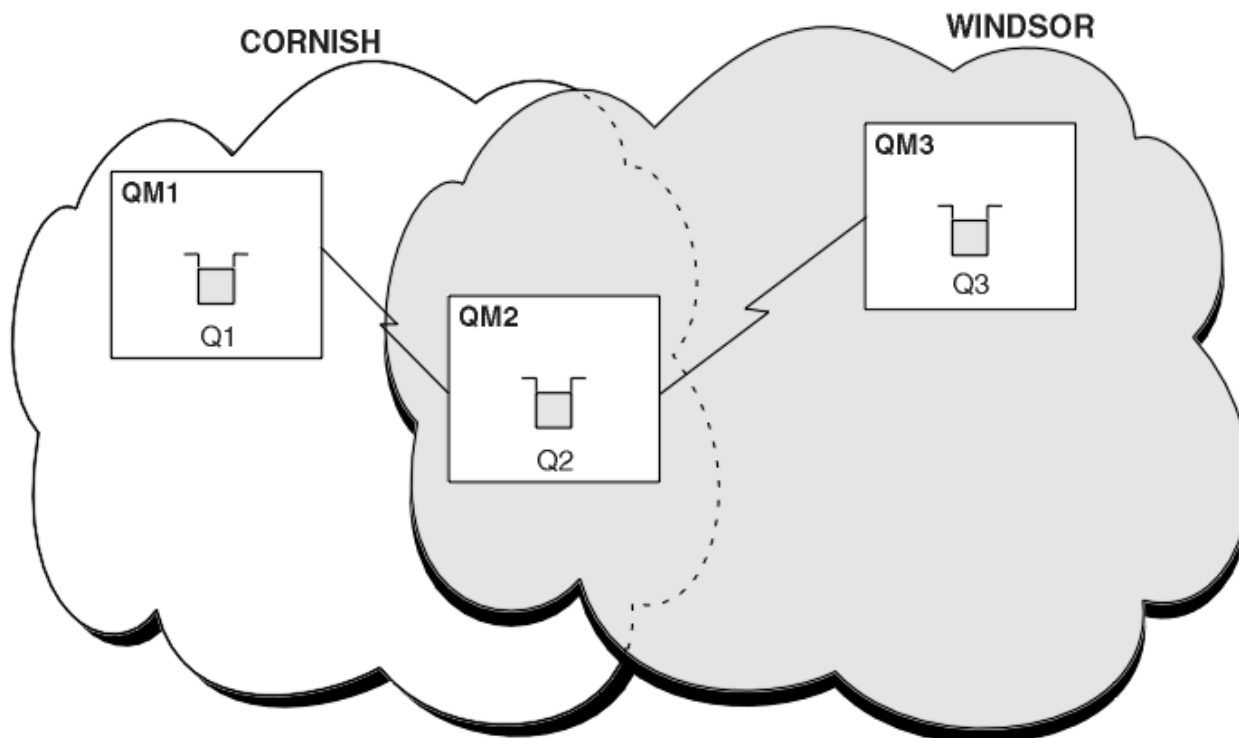
Rozpoznání názvu

Konfigurace cest zpráv mezi klastry

Spojte klastry společně s použitím správce front brány. Učinit fronty nebo správce front viditelné pro všechny klastry definováním aliasů fronty klastru nebo správce front klastru ve správci front brány.

Informace o této úloze

Místo seskupení všech správců front v jednom velkém klastru můžete mít mnoho menších klastrů. Každý klastr má jednoho nebo více správců front, kteří vystupují jako most. Výhodou tohoto je, že můžete omezit viditelnost názvů front a správců front v rámci klastrů. Viz Překrývání klastrů. Chcete-li změnit názvy front a správců front tak, aby nedocházelo ke konfliktům názvů nebo dodržovali lokální konvence pojmenování, použijte aliasy.



Obrázek 58. Přemostění mezi klastry

Produkt Obrázek 58 na stránce 304 zobrazuje dva klastry s mostem mezi nimi. Mohl by existovat více než jeden most.

Nakonfigurujte klastry pomocí následující procedury:

Postup

1. Definujte frontu klastru, Q1 na QM1.

```
DEFINE QLOCAL(Q1) CLUSTER(CORNISH)
```

2. Definujte frontu klastru, Q3 na QM3.

```
DEFINE QLOCAL(Q3) CLUSTER(WINDSOR)
```

3. Vytvořte seznam názvů s názvem CORNISHWINDSOR na QM2 obsahující názvy obou klastrů.

```
DEFINE NAMELIST(CORNISHWINDSOR) DESCR('CornishWindsor namelist')  
NAMES(CORNISH, WINDSOR)
```

4. Definujte frontu klastru, Q2 na QM2

```
DEFINE QLOCAL(Q2) CLUSNL(CORNISHWINDSOR)
```

Jak pokračovat dále

QM2 je členem obou klastrů a je mezi nimi přemostění. Pro každou frontu, kterou chcete zviditelnit přes most, potřebujete definici QALIAS na tomto mostu. Například v produktu [Obrázek 58 na stránce 304](#), v systému QM2, je třeba:

```
DEFINE QALIAS(MYQ3) TARGQ(Q3) CLUSTER(CORNISH) DEFBIND(NOTFIXED)
```

Pomocí aliasu fronty může aplikace připojená ke správci front v produktu CORNISH, například QM1, vložit zprávu do produktu Q3. Odkazuje na Q3 jako MYQ3. Zpráva je směrována na Q3 v QM3.

When you open a queue, you need to set DEFBIND to either NOTFIXED or QDEF. Je-li položka DEFBIND ponechána jako výchozí hodnota OPEN, správce front převede definici aliasu na správce front mostu, který ji hostuje. Most tuto zprávu neodešle.

Pro každého správce front, kterého chcete zviditelnit, je třeba definovat alias správce front. Například v systému QM2 potřebujete:

```
DEFINE QREMOTE(QM1) RNAME(' ') RQMNAME(QM1) CLUSTER(WINDSOR)
```

Aplikace připojená k libovolnému správci front v produktu WINDSOR, například QM3, může vložit zprávu do libovolné fronty na serveru QM1, a to tak, že se explicitně pojmenuje QM1 na volání MQOPEN .

Související pojmy

Alias správce front a klastry

Alias správce front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Alias fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Alias fronty a klastry

Alias fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr

Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Alias správce front a klastry

Alias správce front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Alias správce front, které jsou vytvořeny s použitím definice vzdálených front s mezerou RNAME, mají pět použití:

Přemapování názvu správce front při odesílání zpráv

Alias správce front lze použít k přemapování názvu správce front určeného ve volání MQOPEN na jiného správce front. Může se jednat o správce front klastru. Např. správce front může mít definici alias správce front:

```
DEFINE QREMOTE(YORK) RNAME(' ') RQMNAME(CLUSQM)
```

YORK lze použít jako alias pro správce front s názvem CLUSQM. Když aplikace ve správci front, která provedla tuto definici, vloží zprávu do správce front YORK, lokální správce front tento název vyřeší jako název produktu CLUSQM. Není-li lokální správce front nazván CLUSQM, umístí zprávu do přenosové fronty klastru, která má být přesunuta do CLUSQM. Změní také záhlaví přenosu tak, aby řídíte CLUSQM namísto YORK.

Poznámka: Definice se vztahuje pouze na správce front, který jej provádí. Chcete-li propagovat alias na celý klastr, je třeba přidat atribut CLUSTER do definice vzdálené fronty. Zprávy z jiných správců front, které byly určeny pro produkt YORK, jsou odesílány do produktu CLUSQM.

Změna přenosové fronty nebo určení přenosové fronty při odesílání zpráv

Použití aliasů lze použít k připojení klastru k neklastrovému systému. Například správci front v klastru ITALY mohli komunikovat se správcem front s názvem PALERMO, který je mimo klastr. Chcete-li komunikovat, musí jeden z správců front v klastru vystupovat jako brána. Ve správci front brány zadejte příkaz:

```
DEFINE QREMOTE(ROME) RNAME(' ') RQMNAME(PALERMO) XMITQ(X) CLUSTER(ITALY)
```

Příkaz je definice aliasu správce front. Definuje a inseruje produkt ROME jako správce front, přes který mohou zprávy z libovolného správce front v klastru ITALY dosáhnout svého cíle na PALERMO. Zprávy vkládané do fronty otevřené s názvem správce front nastaveným na hodnotu ROME jsou odeslány správci front brány s definicí aliasu správce front. Jakmile jsou tyto zprávy vloženy do přenosové fronty X a jsou přesunuty neklastrovými kanály do správce front PALERMO.

Výběr názvu ROME v tomto příkladu není významný. Hodnoty pro QREMOTE a RQMNAME mohou být obě stejné.

Určení místa určení při příjmu zpráv

Když správce front přijme zprávu, extrahuje název cílové fronty a správce front z záhlaví přenosu. Pro definici aliasu správce front se stejným názvem, jako má správce front v záhlaví přenosu, hledá alias správce front. Pokud nalezne jeden, nahradí RQMNAME z definice aliasu správce front v záhlaví přenosu za název správce front.

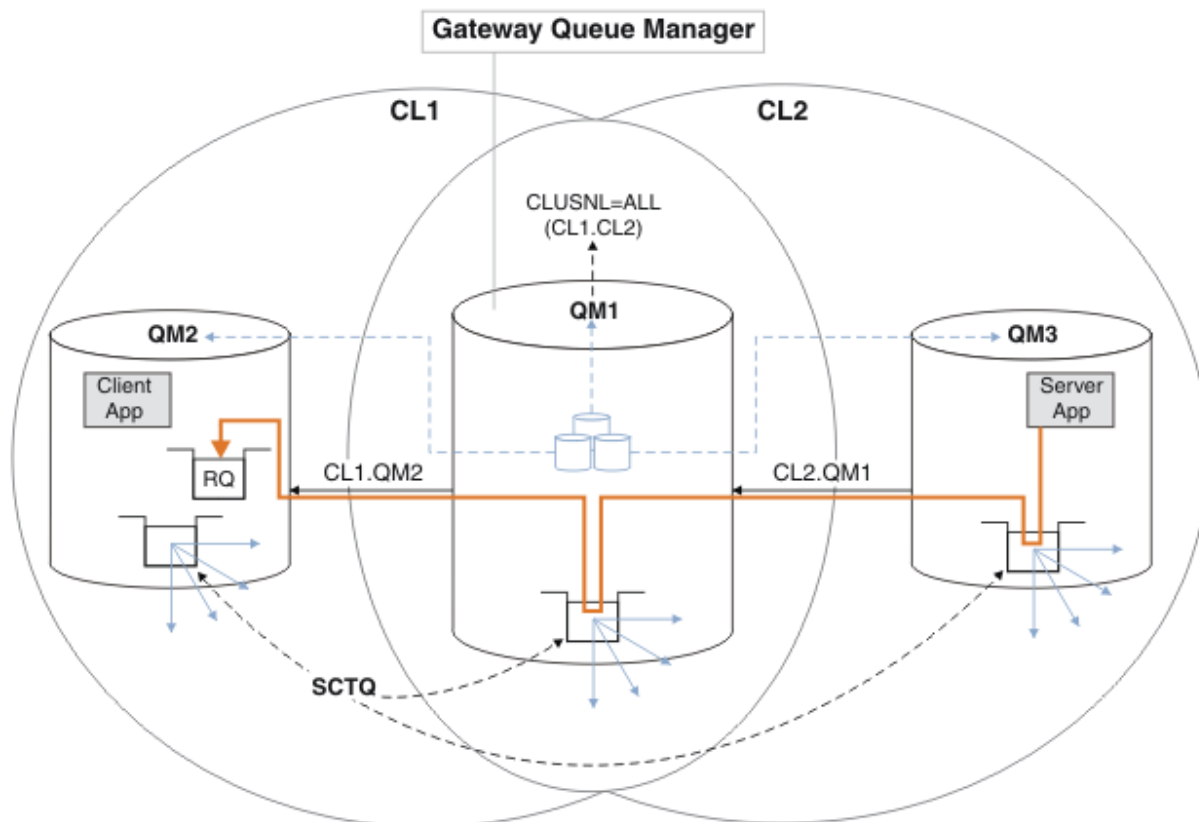
Existují dva důvody pro použití aliasu správce front tímto způsobem:

- Chcete-li směřovat zprávy do jiného správce front
- Chcete-li změnit název správce front tak, aby byl stejný jako lokální správce front, postupujte takto:

Použití aliasů správce front ve správci front brány pro směrování zpráv mezi správci front v různých klastrech.

Aplikace může odeslat zprávu do fronty v jiném klastru pomocí aliasu správce front. Fronta nemusí být frontou klastru. Fronta je definována v jednom klastru. Aplikace je připojena ke správci front v jiném klastru. Správce front brány připojí dva klastry. Není-li fronta definována jako klastrovaná, musí aplikace otevřít frontu za použití názvu fronty a názvu aliasu správce front s klastry. Příklad konfigurace naleznete v části [“Vytvoření dvou překrývajících se klastrů se správcem front brány”](#) na stránce 263, ze které se bere tok zpráv s odpovědí znázorněný na obrázku 1.

Diagram zobrazuje cestu, která byla přijata zprávou odpovědi zpět do dočasné dynamické fronty, která se nazývá RQ. Serverová aplikace připojená k produktu QM3 otevře frontu odpovědi s použitím názvu správce front QM2. Název správce front QM2 je definován jako alias klastrovaného správce front v systému QM1. QM3 směruje zprávu odpovědi na QM1. QM1 směruje zprávu do QM2.



Obrázek 59. Použití aliasu správce front k vrácení zprávy odpovědi do jiného klastru

Způsob práce směrování je následující. Každý správce front v každém klastru má definici aliasu správce front v produktu QM1. Aliasy jsou klastrované ve všech klastrech. Šedé přerušované šipky z každého z aliasů do správce front ukazují, že každý alias správce front je převeden na skutečného správce front alespoň v jednom z klastrů. V tomto případě je alias produktu QM2 klastrovaný v klastru CL1 i v produktu CL2a je interpretován jako skutečný správce front QM2 v produktu CL1. Serverová aplikace vytvoří zprávu s odpovědí pomocí odpovědi na název fronty RQa odpoví na název správce front QM2. Zpráva je směrována na QM1, protože definice aliasu správce front QM2 je definována na QM1 v klastru CL2 a správce front QM2 se nenachází v klastru CL2. Vzhledem k tomu, že zprávu nelze odeslat cílovému správci front, bude odeslána správci front s definicí aliasu.

QM1 umístí zprávu do přenosové fronty klastru v systému QM1 for transferal do QM2. Produkt QM1 směruje zprávu do produktu QM2, protože definice aliasu správce front v produktu QM1 for QM2 definuje QM2 jako skutečného cílového správce front. Definice není cyklická, protože definice aliasů se mohou odkazovat pouze na skutečné definice; alias nemůže odkazovat sám na sebe. Skutečná definice je interpretována produktem QM1, protože se oba QM1 a QM2 nacházejí ve stejném klastru, CL1. Produkt QM1 najde informace o připojení pro produkt QM2 z úložiště pro produkt CL1a směruje

zprávu do produktu QM2. Aby mohla být zpráva přeměrována produktem QM1, serverová aplikace musí mít otevřenou frontu odpovědí s volbou DEFBIND nastavenou na MQBND_BIND_NOT_FIXED. Pokud měla aplikace serveru otevřenou frontu odpovědí s volbou MQBND_BIND_ON_OPEN, zpráva není přeměrována a ukončí se ve frontě nedoručených zpráv.

Použití správce front jako brány v klastru k vyrovnávání pracovní zátěže v důsledku příchodu z mimo klastr.

Definujete frontu s názvem EDINBURGH ve více než jednom správci front v klastru. Chcete, aby klastrový mechanismus vyvažovat pracovní zátěž pro zprávy přicházející do této fronty mimo klastr.

Správce front z prostředí mimo klastr potřebuje pro jednoho správce front v klastru přenosovou frontu a odesílací kanál. Tato fronta se nazývá správce front brány. Chcete-li využít výchozího mechanismu vyrovnávání pracovní zátěže, je třeba použít jedno z následujících pravidel:

- Správce front brány nesmí obsahovat instanci fronty EDINBURGH .
- Správce front brány určuje CLWLUSEQ (ANY) v systému ALTER QMGR.

Příklad vyvažování pracovní zátěže mimo klastr naleznete v tématu [“Konfigurace vyrovnávání pracovní zátěže mimo klastr”](#) na stránce 301 .

Související pojmy

Alias fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Alias fronty a klastry

Alias fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr

Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skryté podrobnosti o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry

Spojte klastry společně s použitím správce front brány. Učinit fronty nebo správce front viditelné pro všechny klastry definováním aliasů fronty klastru nebo správce front klastru ve správci front brány.

Alias fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Příklad:

- Aplikace ve správci front VENICE odešle zprávu do správce front PISA pomocí volání MQPUT . Aplikace poskytuje v deskriptoru zpráv následující informace o odpovědi na frontu:

```
ReplyToQ=' QUEUE '  
ReplyToQMgi=' '
```

- Aby mohly být odpovědi odeslané do produktu QUEUE přijaty v produktu OTHERQ na PISA, vytvořte definici vzdálené fronty v systému VENICE , která se používá jako alias fronty pro odpověď. Alias je účinný pouze na systému, na kterém byl vytvořen.

```
DEFINE QREMOTE(Queue) RNAME(OTHERQ) RQMNAME(PISA)
```

RQMNAME a QREMOTE mohou určovat stejné názvy, a to i v případě, že RQMNAME je sám správcem front klastru.

Související pojmy

Alias správců front a klastrů

Alias správců front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Alias fronty a klastrů

Alias fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr

Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skryté podrobnosti o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry

Spojte klastry společně s použitím správce front brány. Učinit fronty nebo správce front viditelné pro všechny klastry definováním aliasů fronty klastru nebo správce front klastru ve správci front brány.

Alias fronty a klastrů

Alias fronty použijte ke skrytí názvu fronty klastru, ke klastru fronty, k převzetí různých atributů nebo k převzetí různých řízení přístupu.

Definice QALIAS se používá k vytvoření aliasu, podle kterého má být známa fronta. Alias můžete vytvořit z mnoha důvodů:

- Chcete začít používat jinou frontu, ale nechcete měnit své aplikace.
- Nechcete, aby aplikace znali skutečné jméno fronty, do které zprávy umisťují.
- Můžete mít konvenci pojmenování, která se liší od definice fronty, kde je fronta definována.
- Vaše aplikace nemusí být autorizovány pro přístup ke frontě podle jejího skutečného názvu, ale pouze pomocí aliasu.

Vytvořte definici QALIAS ve správci front pomocí příkazu DEFINE QALIAS . Spustte například příkaz:

```
DEFINE QALIAS(PUBLIC) TARGQ(LOCAL) CLUSTER(C)
```

Tento příkaz oznámí frontu s názvem PUBLIC správci front v klastru C. PUBLIC je alias, který se interpretuje na frontu s názvem LOCAL. Zprávy odeslané do PUBLIC jsou směrovány do fronty s názvem LOCAL.

K rozlišení názvu fronty do fronty klastru můžete také použít definici alias fronty. Spustte například příkaz:

```
DEFINE QALIAS(PRIVATE) TARGQ(PUBLIC)
```

Tento příkaz umožňuje správci front použít název PRIVATE k přístupu do fronty oznámené jinde v klastru názvem PUBLIC. Protože tato definice nezahrnuje atribut CLUSTER, vztahuje se pouze na správce front, který jej činí.

Související pojmy

Alias správce front a klastry

Alias správce front použijte ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Alias fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Související úlohy

Konfigurace požadavku/odpovědi na klastr

Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.


Konfigurace cest zpráv mezi klastry

Spojte klastry společně s použitím správce front brány. Učinit fronty nebo správce front viditelné pro všechny klastry definováním aliasů fronty klastru nebo správce front klastru ve správci front brány.

Použití klastrů pro správu pracovní zátěže

Definováním více instancí fronty v různých správcích front v klastru můžete šířit práci obsluhy fronty na více serverech. Existuje několik faktorů, které mohou zabránit opětnému zařazení zpráv do jiného správce front v případě selhání.


Kromě nastavení klastrů za účelem snížení administrace systému můžete vytvořit klastry, ve kterých bude více než jeden správce front hostitelem instance stejné fronty.

Můžete uspořádat klastr tak, aby byli správci front v sobě klonovány. Každý správce front je schopen spouštět stejné aplikace a mít lokální definice stejných front.  Příklad: V paralelním prostředí sysplex produktu z/OS mohou klonované aplikace přistupovat k datům ve sdílené databázi Db2 nebo v databázi VSAM (Virtual Storage Access Method). Pracovní zátěž mezi správci front můžete rozložit tak, že budete mít několik instancí určité aplikace. Každá instance aplikace přijímá zprávy a spouští se nezávisle na ostatních.

Výhody použití klastrů tímto způsobem jsou následující:

- Zvýšená dostupnost front a aplikací.
- Rychlejší propustnost zpráv.
- Více rozložení pracovní zátěže ve vaší síti.

Každý správce front, který je hostitelem instance určité fronty, může zpracovávat zprávy určené pro danou frontu a aplikace nepojmenují správce front při odesílání zpráv. Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být směrována zpráva. Vhodné cíle jsou zvoleny na základě dostupnosti správce front a fronty a na určitém počtu atributů specifických pro pracovní zátěž klastru, které jsou přidruženy ke správcům front, frontám a kanálům. Viz [Vyrovnávání pracovní zátěže v klastrech](#).

 V produktu IBM MQ for z/OS mohou správci front, kteří jsou ve skupině sdílení front, hostit fronty klastru jako sdílené fronty. Sdílené fronty klastru jsou k dispozici pro všechny správce front ve stejné skupině sdílení front. For example, in [Klastr s více instancemi stejné fronty](#), either or both of the

queue managers QM2 and QM4 can be a shared-queue manager. Každý má definici pro frontu Q3. Kterýkoli z správců front ve stejné skupině sdílí front jako produkt QM4 může číst zprávu vkládanou do sdílené fronty Q3. Každá skupina sdílení front může obsahovat až 32 správců front, přičemž každý z nich má přístup ke stejným datům. Sdílení fronty výrazně zvyšuje propustnost vašich zpráv.

Další informace o konfiguracích klastru pro správu pracovní zátěže naleznete v následujících dílčích tématech:

Související pojmy

[“Směrování zpráv do a z klastrů” na stránce 293](#)

Aliases fronty, aliasy správců front a definice vzdálených front slouží k připojení klastrů k externím správcům front a dalším klastrům.

Související úlohy

[“Konfigurace klastru správce front” na stránce 216](#)

Klastry poskytují mechanismus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

[“Nastavení nového klastru” na stránce 228](#)

Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

[“Konfigurace vyrovnávání pracovní zátěže mimo klastr” na stránce 301](#)

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Související informace

[Porovnání klastrování a distribuovaných front](#)

[Distribuované fronty a klastry](#)

[Komponenty klastru](#)

[Kanály klastru](#)

[Co se stane, pokud je fronta klastru zakázána pro MQPUT](#)

[Vyrovnávání pracovní zátěže nastavené na odesílacím kanálu klastru nefunguje.](#)

[Ukázkový program pro monitorování front klastru \(AMQSCLM\)](#)

[Zápis a kompilace uživatelských procedur pracovní zátěže klastru](#)

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

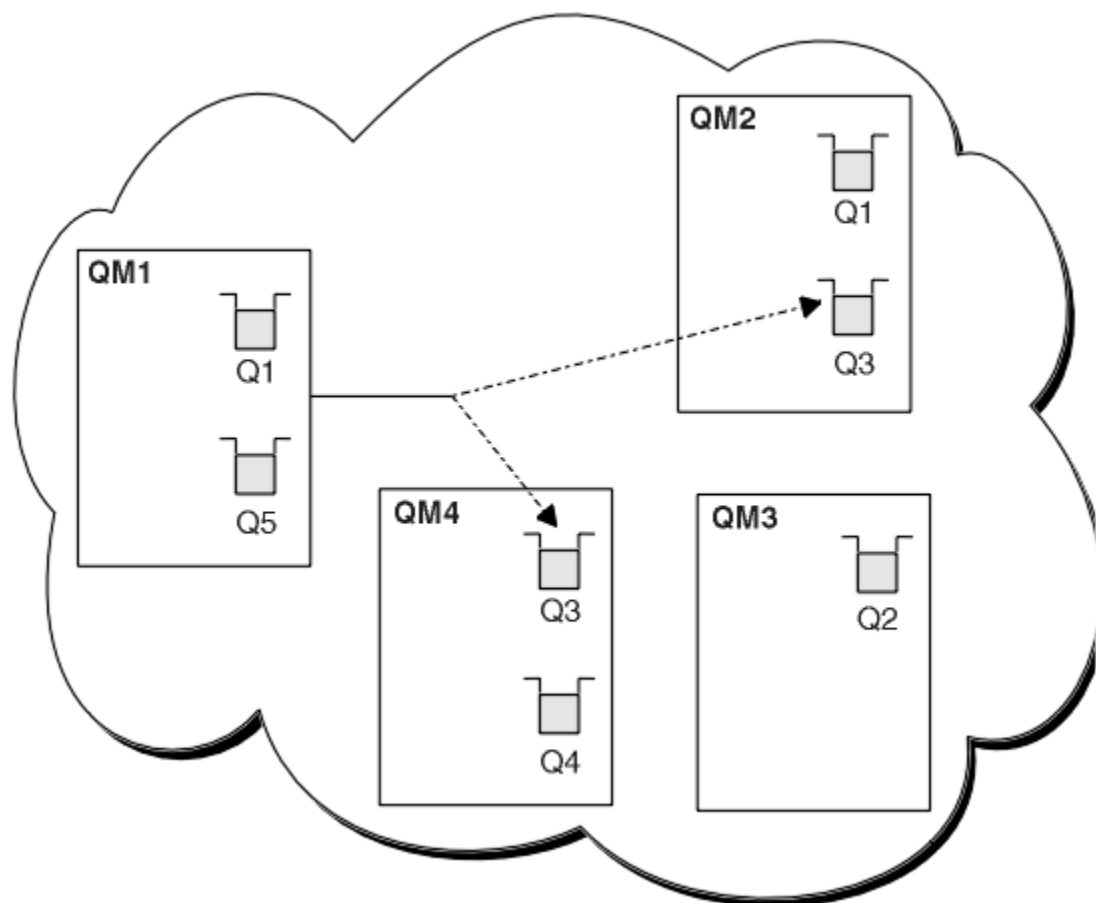
[Obrázek 60 na stránce 312](#) ukazuje klastr, v němž je pro frontu Q3 více než jedna definice. Pokud aplikace v produktu QM1 vloží zprávu do produktu Q3, nemusí nutně vědět, která instance produktu Q3 bude zpracovávat svou zprávu. Je-li aplikace spuštěna na serveru QM2 nebo v produktu QM4, kde jsou lokální instance produktu Q3, je lokální instance produktu Q3 standardně otevřena. Nastavením atributu fronty CLWLUSEQ lze lokální instanci fronty považovat stejně jako vzdálenou instanci fronty.

Volba MQOPEN DefBind řídí, zda je cílový správce front vybrán při vyvolání volání MQOPEN, nebo když je zpráva přenesena z přenosové fronty.

Nastavíte-li volbu DefBind na hodnotu MQBND_BIND_NOT_FIXED, lze zprávu odeslat na instanci fronty, která je k dispozici při přenosu zprávy. Tím se vyvarujete následujících problémů:

- Pokud zpráva dorazí do cílového správce front, není cílová fronta k dispozici.
- Stav fronty se změnil.
- Zpráva byla vložena pomocí aliasu fronty klastru a ve správcí front neexistuje žádná instance cílové fronty, ve které je definována instance aliasu fronty klastru.

Jsou-li tyto problémy zjištěny v čase přenosu, je požadována jiná dostupná instance cílové fronty a zpráva je přeměrována. Nejsou-li k dispozici žádné instance fronty, bude zpráva umístěna do fronty nedoručených zpráv.



Obrázek 60. Klastř s více instancemi stejné fronty.

Jedním z faktorů, které mohou zabránit přeměrování zpráv, je, že zprávy byly přiřazeny k opravenému správci front nebo kanálu s volbou MQBND_BIND_ON_OPEN. Zprávy, které jsou svázané s produktem MQOPEN, nejsou nikdy znovu přiděleny jinému kanálu. Všimněte si také, že k opětovnému přidělení zpráv dochází pouze tehdy, když se kanál klastř skutečně nedaří. K opětovné alokaci nedojde v případě, že kanál již selhal.

Systém se pokusí přeměrovat zprávu v případě, že správce cílových front přestane pracovat. Tímto způsobem neovlivní integritu zprávy tím, že se spustí riziko ztráty nebo vytvoření duplikátu. Pokud správce front selže a zanechá zprávu v nejistém stavu, tato zpráva není přeměrována.

z/OS V systému IBM MQ for z/OS nedojde k úplnému zastavení kanálu, dokud nedojde k dokončení procesu nového přidělení zprávy. Zastavení kanálu s režimem nastaveným na hodnotu FORCE nebo TERMINATE přeruší proces, takže pokud tak učiníte, mohou být některé zprávy BIND_NOT_FIXED již přerozděleny do jiného kanálu nebo mohou být zprávy mimo pořadí.

Poznámka: **z/OS**

1. Před nastavením klastř, který má více instancí stejné fronty, zajistěte, aby vaše zprávy neměly závislosti na sobě navzájem. Například je třeba, aby byly zpracovány v určité posloupnosti nebo ve stejném správci front.
2. Učinit definice pro různé instance stejné fronty identické. Jinak získáte odlišné výsledky z různých volání MQINQ.

Související pojmy

[Programování aplikací a klastř](#)

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klaster INVENTORY byl nastaven tak, jak je popsáno v tématu Přidání nového správce front do klastru. Obsahuje tři správce front; produkty LONDON a NEWYORK obsahují úplná úložiště, produkt PARIS uchovává dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK . Aplikace je řízena doručení zpráv ve frontě INVENTQ .
- Chceme přidat instanci produktu INVENTQ , která poskytuje dodatečnou kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Informace o této úloze

Chcete-li přidat správce front, který je hostitelem fronty lokálně, postupujte podle následujících kroků.

Postup

1. Změňte správce front produktu PARIS .

Aby aplikace v Paříži používala INVENTQ v Paříži a v New Yorku, musíme o tom informovat správce front. V systému PARIS zadejte následující příkaz:

```
ALTER QMGR CLWLUSEQ (ANY)
```

2. Přezkoumejte aplikaci soupisu pro afinity zpráv.

Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv. Další informace najdete v tématu [Práce s spřízněnostmi zpráv](#).

3. Instalovat inventární aplikaci na systém v Paříži.
4. Definujte frontu klastru INVENTQ.

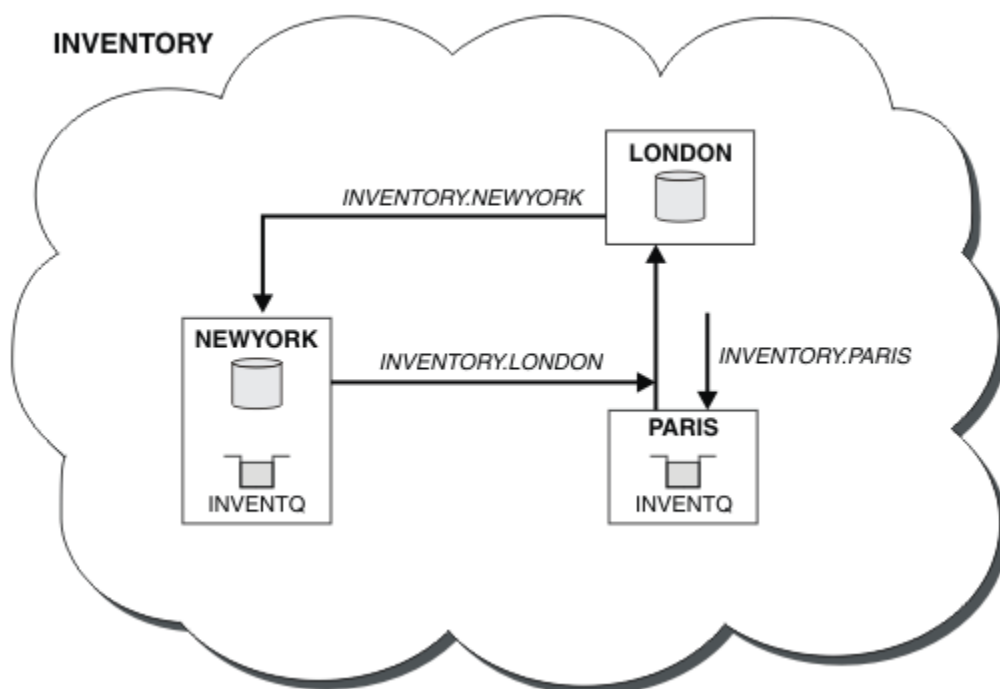
Frontu INVENTQ, která je již hostována správcem front NEWYORK, je také hostována pomocí PARIS. Definujte jej ve správci front produktu PARIS takto:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front PARIS. Listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 61 na stránce 314 zobrazuje klastr nastavený touto úlohou.



Obrázek 61. Klastr INVENTORY se třemi správci front

Úpravy tohoto klastru byly provedeny bez změny správců front NEWYORK nebo LONDON. Úplná úložiště v těchto správci front jsou aktualizována automaticky s informacemi, které potřebují k odesílání zpráv do produktu INVENTQ na adrese PARIS.

Jak pokračovat dále

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správci front v klastru. To zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje distribuci pracovní zátěže mezi dvěma správci front. Zprávy ukládané do INVENTQ některým ze správců front LONDON, NEWYORK, PARIS jsou směrovány střídavě na PARIS nebo NEWYORK, takže pracovní zátěž je vyvážená.

Související pojmy

[Příklad klastru s více než jednou instancí fronty](#)

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klaster INVENTORY byl nastaven tak, jak je popsáno v tématu "Přidání správce front do klastru". Obsahuje tři správce front; produkty LONDON a NEWYORK obsahují úplná úložiště, produkt PARIS uchovává dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK . Aplikace je řízena doručením zpráv ve frontě INVENTQ .
- Do produktu TOKYO se přidává nové úložiště, kde jsou dvě různé sítě. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Informace o této úloze

Chcete-li používat dvě sítě v klastru, postupujte takto.

Postup

1. Rozhodněte se, které úplné úložiště TOKYO odkazuje na první.

Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Staví své vlastní dílčí úložiště. To není zvláštní význam, který úložiště si vyberete. V tomto příkladě je vybrána volba NEWYORK . Poté, co se nový správce front připojí ke klastru, komunikuje s oběma úložišti.

2. Definujte kanály CLUSRCVR .

Každý správce front v klastru musí definovat příjemce klastru, na kterém může přijímat zprávy. Tento správce front musí být schopen komunikovat na každé síti.

```
DEFINE CHANNEL(INVENTORY.TOKYO.NETB) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNNAME('TOKYO.NETB.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
channel using network B for TOKYO')
```

```
DEFINE CHANNEL(INVENTORY.TOKYO.NETA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNNAME('TOKYO.NETA.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
channel using network A for TOKYO')
```

3. Definujte kanál CLUSSDR ve správci front TOKYO.

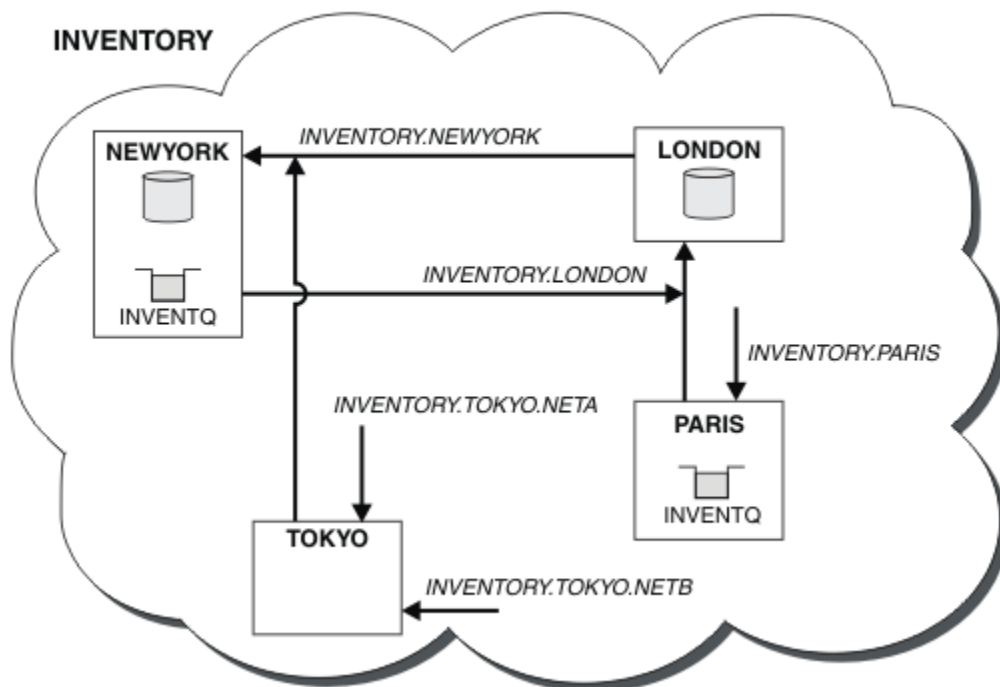
Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK, takže TOKYO potřebuje následující definici:

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-sender
channel from TOKYO to repository at NEWYORK')
```

Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front PARIS. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 62 na stránce 316 zobrazuje klastr nastavený touto úlohou.



Obrázek 62. Klastr INVENTORY se čtyřmi správci front

Při vytváření pouze tří definic jsme přidali správce front TOKYO do klastru se dvěma různými dostupnými přenosovými cestami k síti.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

“Přidání správce front do klastru” na stránce 238

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí jedné přenosové fronty klastru SYSTEM . CLUSTER . TRANSMIT . QUEUE.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastř INVENTORY byl nastaven tak, jak je popsáno v tématu “Použití dvou sítí v klastru” na stránce 315. Obsahuje čtyři správce front; LONDON a NEWYORK drží úplná úložiště; PARIS a TOKYO uchovávají dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK. Správce front produktu TOKYO má dvě různé sítě, na kterých může komunikovat.
- Chcete vytvořit jednu ze sítí na primární síti a jinou síť ze záložní sítě. Máte v plánu použít záložní síť, pokud existuje problém s primární sítí.

Informace o této úloze

Atribut NETPRTY použijte ke konfiguraci primární a sekundární sítě v klastru.

Postup

Změňte existující kanály CLUSRCVR na systému TOKYO.

Chcete-li označit, že kanál je primární kanál a kanál B kanál je sekundární kanál, použijte následující příkazy:

- a) ALTER CHANNEL(INVENTORY.TOKYO.NETA) CHLTYPE(CLUSRCVR) NETPRTY(2) DESCR('Main cluster-receiver channel for TOKYO')
- b) ALTER CHANNEL(INVENTORY.TOKYO.NETB) CHLTYPE(CLUSRCVR) NETPRTY(1) DESCR('Backup cluster-receiver channel for TOKYO')

Jak pokračovat dále

Konfigurací kanálu s různými prioritami sítě jste nyní definovali klastr, který má primární síť a sekundární síť. Správci front v klastru, kteří používají tyto kanály, automaticky používají primární síť, pokud jsou k dispozici. Pokud primární síť není k dispozici, správci front se v případě, že nejsou k dispozici primární síť, mohou používat sekundární síť.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 238. Obsahuje tři správce front; produkty LONDON a NEWYORK obsahují úplná úložiště, produkt PARIS uchovává dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK . Aplikace je řízena doručení zpráv ve frontě INVENTQ .

- Probíhá vytváření nového úložiště v Chicagu za účelem poskytnutí zálohy pro systém inventáře, který se nyní spouští v New Yorku. Chicagský systém se používá pouze v případě, že je problém s New Yorkem.

Informace o této úloze

Chcete-li přidat frontu, která bude sloužit jako záloha, postupujte takto.

Postup

1. Rozhodněte se, které úplné úložiště CHICAGO odkazuje na první.

Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Staví své vlastní dílčí úložiště. Nemá zvláštní význam, které úložiště si vyberete pro konkrétního správce front. V tomto příkladě je vybrána volba NEWYORK . Poté, co se nový správce front připojil ke klastru, komunikuje s oběma úložišti.

2. Definujte kanál CLUSRCVR .

Každý správce front v klastru musí definovat příjemce klastru, na kterém může přijímat zprávy. V systému CHICAGO definujte:

```
DEFINE CHANNEL (INVENTORY.CHICAGO) CHLTYPE (CLUSRCVR) TRPTYPE (TCP)
CONNAME (CHICAGO.CMSTORE.COM) CLUSTER (INVENTORY) DESCR ('Cluster-receiver
channel for CHICAGO')
```

3. Definujte kanál CLUSSDR ve správci front CHICAGO.

Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK, takže CHICAGO potřebuje následující definici:

```
DEFINE CHANNEL (INVENTORY.NEWYORK) CHLTYPE (CLUSSDR) TRPTYPE (TCP)
CONNAME (NEWYORK.CHSTORE.COM) CLUSTER (INVENTORY) DESCR ('Cluster-sender
channel from CHICAGO to repository at NEWYORK')
```

4. Změňte existující frontu klastru INVENTQ.

Hlavní instancí fronty je produkt INVENTQ , který je již hostitelem správce front NEWYORK .

```
ALTER QLOCAL (INVENTQ) CLWLPRTY (2)
```

5. Přejete-li si aplikaci soupisu pro afinity zpráv.

Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv.

6. Nainstalujte inventární aplikaci na systém v produktu CHICAGO.

7. Definujte záložní frontu klastru INVENTQ

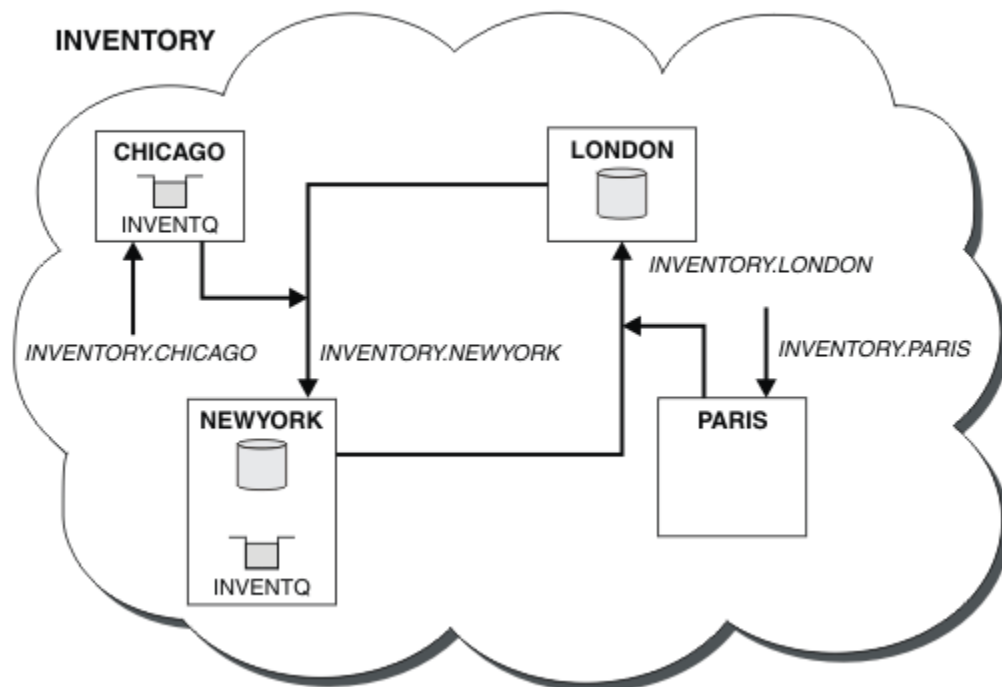
Server INVENTQ , který je již hostován správcem front NEWYORK , je také hostován jako záloha pomocí CHICAGO. Definujte jej ve správci front produktu CHICAGO takto:

```
DEFINE QLOCAL (INVENTQ) CLUSTER (INVENTORY) CLWLPRTY (1)
```

Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front CHICAGO. Program modulu listener naslouchá přichozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

[Obrázek 63 na stránce 320](#) zobrazuje klastr nastavený touto úlohou.



Obrázek 63. Klastř INVENTORY se čtyřmi správci front

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správcích front v klastř. Správce front produktu CHICAGO je zálohou. Zprávy odeslané do INVENTQ jsou směřovány na NEWYORK, pokud nejsou k dispozici, když jsou odeslány do CHICAGO.

Poznámka:

Dostupnost vzdáleného správce front je založena na stavu kanálu s daným správcem front. Když se kanály spustí, jejich stav se změní několikrát, přičemž některé z těchto stavů jsou méně přednostní pro algoritmus správy pracovní zátěže klastř. V praxi to znamená, že lze zvolit nižší prioritu (záložní) místa určení, zatímco se spouští kanály pro vyšší prioritu (primární) cíle.

Potřebujete-li zajistit, aby žádné zprávy nepřešli na místo určení zálohování, nepoužívejte CLWLPRTY. Zvažte použití samostatných front nebo příkazu CLWLRANK s ručním přepíděním z primárního zálohování.

Související pojmy

Příklad klastř s více než jednou instancí fronty

V tomto příkladu klastř s více než jednou instancí fronty jsou zprávy směřovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastř

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ, abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastř

Chcete-li přidat nové úložiště v produktu TOKYO, kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastř

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Aplikace pro kontrolu cen musí být nainstalována na různých správcích front. Počet kanálů, které jsou používány k nízkému počtu kanálů, je omezeno tím, že je omezen počet aktivních kanálů každého serveru. Aplikace je řízena doručením zpráv ve frontě PRICEQ .
- Čtyři správci front serveru hostí aplikaci kontroly cen. Dva správci front dotazů odesílají zprávy do produktu PRICEQ za účelem zadání dotazu na cenu. Dva další správci front jsou konfigurováni jako úplná úložiště.

Informace o této úloze

Chcete-li omezit počet použitých kanálů, postupujte takto.

Postup

1. Vyberte dvě úplná úložiště.

Zvolte dva správce front, kteří budou úplnými úložišti pro váš klastr kontroly cen. Nazývaly se REPOS1 a REPOS2.

Spusťte následující příkaz:

```
ALTER QMGR REPOS (PRICECHECK)
```

2. Definujte kanál CLUSRCVR pro každého správce front.

V každém správci front v klastru definujte kanál příjemce klastru a odesílací kanál klastru. Nezáleží na tom, která definice je definována jako první.

```
DEFINE CHANNEL (PRICECHECK.SERVE1) CHLTYPE (CLUSRCVR) TRPTYPE (TCP)  
CONNNAME (SERVER1.COM) CLUSTER (PRICECHECK) DESCR ('Cluster-receiver channel')
```

3. Definujte kanál CLUSSDR pro každého správce front.

Vytvořte v každém správci front definici CLUSSDR a propojte tohoto správce front s jedním nebo více správci front úplného úložiště.

```
DEFINE CHANNEL (PRICECHECK.REPOS1) CHLTYPE (CLUSSDR) TRPTYPE (TCP)  
CONNNAME (REPOS1.COM) CLUSTER (PRICECHECK) DESCR ('Cluster-sender channel to  
repository queue manager')
```

4. Nainstalujte aplikaci kontroly cen.
5. Definujte frontu PRICEQ ve všech správcích front serveru.

Vydejte následující příkaz pro každý z nich:

```
DEFINE QLOCAL (PRICEQ) CLUSTER (PRICECHECK)
```

6. Omezit počet kanálů používaných dotazy

Na správcích front dotazů omezujeme počet používaných aktivních kanálů, a to zadáním následujících příkazů pro každou z těchto možností:

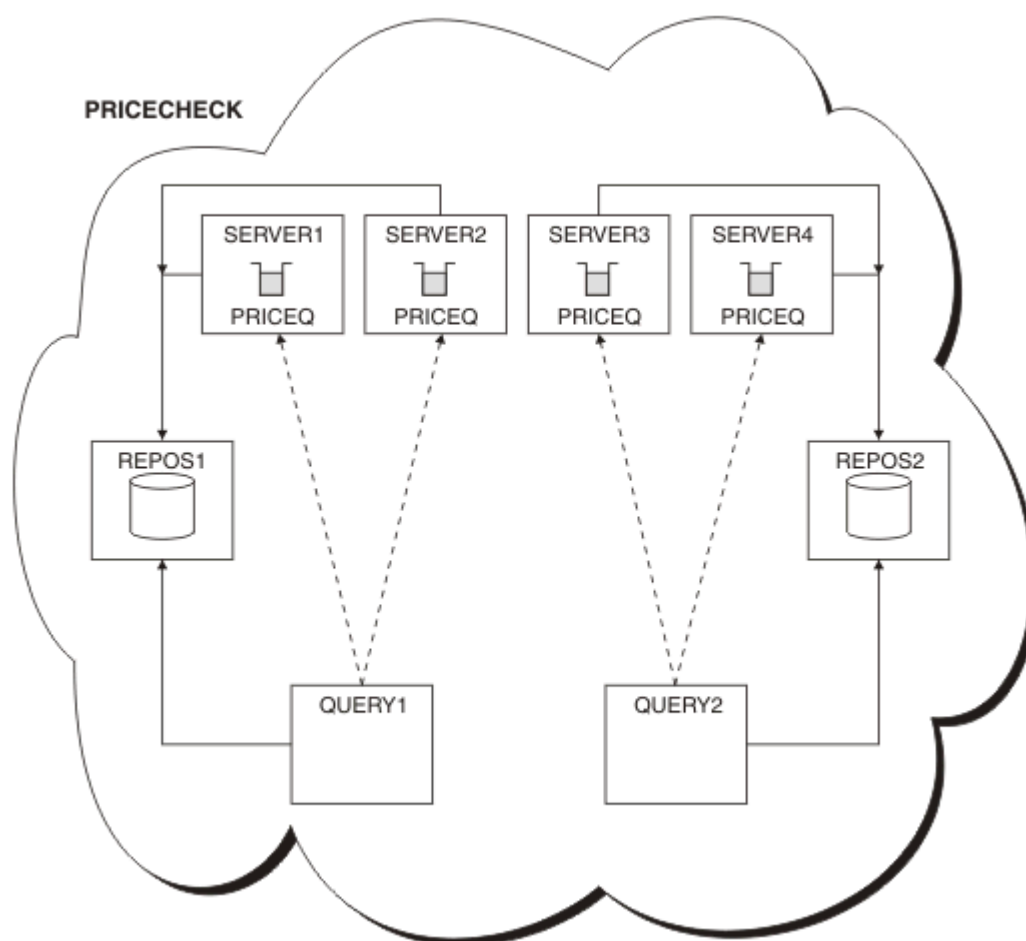
```
ALTER QMGR CLWLMRUC (2)
```

7. Pokud jste tak dosud neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener.

Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 64 na stránce 322 zobrazuje klastr nastavený touto úlohou.



Obrázek 64. Klastr PRICECHECK se čtyřmi správci front serveru, dvěma úložišti a dvěma správci front dotazů.

Ačkoli jsou v klastru PRICECHECK k dispozici čtyři instance fronty produktu PRICEQ, každý dotazovací správce front používá pouze dva dva z nich. Správce front produktu QUERY1 má například pouze aktivní kanály pro správce front SERVER1 a SERVER2. Pokud se produkt SERVER1 stane nedostupným, správce front produktu QUERY1 by pak mohl začít používat jiného správce front, například SERVER3.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klaster INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 238. Obsahuje tři správce front: LONDON a NEWYORK udržují úplná úložiště, PARIS ukládá dílčí úložiště a umísťuje zprávy z produktu INVENTQ. Aplikace soupisu se spustí na systému v New Yorku připojeném ke správci front NEWYORK . Aplikace je řízena doručením zpráv ve frontě INVENTQ .
- V Los Angeles je vytvářený nový obchod. Chcete-li poskytnout dodatečnou kapacitu, chcete spustit systém inventářů v Los Angeles stejně jako New York. Nový správce front může zpracovat dvakrát tolik zpráv jako New York.

Informace o této úloze

Chcete-li přidat výkonnějšího správce front, který je hostitelem fronty, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště LOSANGELES odkazuje na první.

2. Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Staví své vlastní dílčí úložiště. To není zvláštní význam, který úložiště si vyberete. V tomto příkladě je vybrána volba NEWYORK . Poté, co se nový správce front připojil ke klastru, komunikuje s oběma úložišti.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from LOSANGELES to repository at NEWYORK')
```

3. Definujte kanál CLUSRCVR ve správci front LOSANGELES.

Každý správce front v klastru musí definovat kanál příjemce klastru, ve kterém může přijímat zprávy. V systému LOSANGELESdefinujte:

```
DEFINE CHANNEL(INVENTORY.LOSANGELES) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNNAME(LOSANGELES.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-receiver channel for queue manager LOSANGELES')
CLWLWGHT(2)
```

Přijímací kanál klastru oznamuje dostupnost zpráv od jiných správců front v klastru INVENTORY. Nastavení CLWLWGHT na dva zajistí, že správce front v Los Angeles dostane dvakrát tolik zpráv o inventuře jako New York (je-li kanál pro NEWYORK nastaven na hodnotu jedna).

4. Upravte kanál CLUSRCVR ve správci front NEWYORK.

Ujistěte se, že správce front v Los Angeles dostane dvakrát tolik inventárních zpráv jako New York. Upravte definici přijímacího kanálu klastru.

```
ALTER CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) CLWLWGHT(1)
```

5. Přezkoumejte aplikaci soupisu pro afinity zpráv.

Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv.

6. Instalovat inventární aplikaci na systém v Los Angeles

7. Definujte frontu klastru INVENTQ.

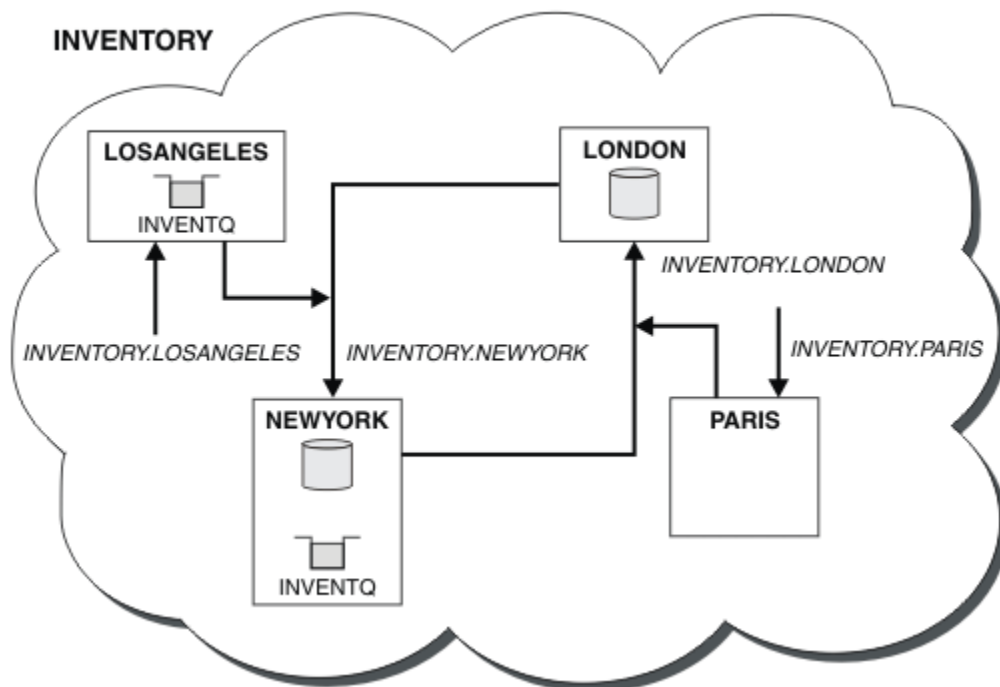
Frontu INVENTQ , která je již hostována správcem front NEWYORK , je také hostována pomocí LOSANGELES. Definujte jej ve správci front produktu LOSANGELES takto:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front LOSANGELES. Program modulu listener naslouchá přichozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

“Přidání výkonnějšího správce front, který je hostitelem fronty” na stránce 323 zobrazuje klastr nastavený touto úlohou.



Obrázek 65. Klastř INVENTORY se čtyřmi správci front

Tato úprava klastř byla dokončena, aniž byste museli měnit správce front LONDON a PARIS. Úložiště v těchto správci front jsou automaticky aktualizována informacemi, které potřebují k odesílání zpráv do produktu INVENTQ na adrese LOSANGELES.

Jak pokračovat dále

Fronta produktu INVENTQ a katalogizace jsou hostovány na dvou správci front v klastř. Konfigurace zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje distribuci pracovní zátěže mezi dvěma správci front. Zprávy, které byly do produktu INVENTQ vloženy buď pomocí produktu LOSANGELES, nebo NEWYORK, jsou zpracovávány instancí v lokální správci front, kdykoli je to možné. Zprávy zařazené do LONDON nebo PARIS jsou směřovány na LOSANGELES nebo NEWYORK, dvakrát tolik zpráv, které se posílají na LOSANGELES.

Související pojmy

Příklad klastř s více než jednou instancí fronty

V tomto příkladu klastř s více než jednou instancí fronty jsou zprávy směřovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správci front.

Programování aplikací a klastř

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ, abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastř

Chcete-li přidat nové úložiště v produktu TOKYO, kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správci front v Tokiu.

Použití primární a sekundární sítě v klastř

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Aplikace mohou otevřít frontu pomocí volání MQOPEN . Aplikace používají volání MQPUT k vložení zpráv do otevřené fronty. Aplikace mohou vložit jednu zprávu do fronty, která ještě není otevřená, pomocí volání MQPUT1 .

Pokud jste nastavili klastry, které mají více instancí stejné fronty, neexistují žádné specifické pokyny pro programování aplikací. Chcete-li však využívat výhody správy pracovní zátěže pro klastrování, může být zapotřebí upravit vaše aplikace. Pokud jste nastavili síť, ve které existuje více definic stejné fronty, přezkoumejte své aplikace pro zprávy s afinitními zprávami.

Předpokládejme například, že máte dvě aplikace, které se spoléhají na posloupnost zpráv, které mezi nimi proudí ve formě otázek a odpovědí. Pravděpodobně budete chtít odpovědi vrátit se zpět na stejného správce front, který odeslal otázku. Je důležité, aby rutina správy pracovní zátěže neodeslala žádné zprávy do žádného správce front, který je hostitelem kopie fronty odpovědí.

Můžete mít aplikace, které vyžadují zpracování zpráv v posloupnosti (například aplikace replikace databáze, která odesílá dávky zpráv, které musí být načteny v posloupnosti). Použití segmentovaných zpráv může také způsobit problém afinity.

Otevření lokální nebo vzdálené verze cílové fronty

Uvědomte si, jak správce front zvolí, zda má být použita lokální nebo vzdálená verze cílové fronty.

1. Správce front otevře lokální verzi cílové fronty pro čtení zpráv nebo pro nastavení atributů fronty.
2. Správce front otevře jakoukoli instanci cílové fronty pro zápis zpráv, je-li splněna alespoň jedna z následujících podmínek:
 - Lokální verze cílové fronty neexistuje.
 - Správce front uvádí CLWLUSEQ (ANY) v systému ALTER QMGR.
 - Fronta ve správci front uvádí CLWLUSEQ (ANY).

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Práce s afinitními zprávami

Afinity zpráv jsou zřídka součástí dobrého návrhu programování. Chcete-li plně využívat klastrování, je třeba odstranit afinity zpráv. Pokud nemůžete odebrat afinity zpráv, můžete vynutit doručení souvisejících zpráv pomocí stejného kanálu a stejného správce front.

Máte-li aplikace se spřízněnostmi zpráv, odeberte před spuštěním použití klastrů afinity.

Odebrání afinit zpráv zvyšuje dostupnost aplikací. Aplikace odešle dávku zpráv s afinními ke správci front. Správce front selže po přijetí pouze části dávky. Odesílající správce front musí před odesláním dalších zpráv čekat na zotavení a zpracování nedokončené dávky zpráv.

Odebrání afinit zpráv zlepšuje také rozšiřitelnost aplikací. Dávkové zpracování zpráv s afinními může zamknout prostředky v cílovém správci front během čekání na následné zprávy. Tyto prostředky mohou zůstat zamčené po dlouhou dobu, čímž brání ostatním aplikacím ve své práci.

Kromě toho afinity zpráv brání tomu, aby rutiny správy pracovní zátěže klastru mohly provádět nejlepší volbu správce front.

Chcete-li odstranit afinity, zvažte následující možnosti:

- Přenášení informací o stavu ve zprávách
- Udržování informací o stavu v nestabilním úložišti přístupném pro libovolného správce front, například v databázi Db2
- Replikace dat jen pro čtení tak, aby byla přístupná více než jednomu správci front

Pokud není vhodné upravit vaše aplikace tak, aby byly odstraněny afinity zpráv, je k dispozici řada možných řešení problému.

Zadat název určitého místa určení ve volání MQOPEN

Zadejte název vzdálené fronty a název správce front v každém volání produktu MQOPEN a všechny zprávy zařazené do fronty používající tento manipulátor objektu jsou odesílány ke stejnému správci front, což může být lokální správce front.

Zadání názvu vzdálené fronty a názvu správce front pro každé volání MQOPEN má nevýhody:

- Není prováděno žádné vyrovnávání pracovní zátěže. Nevyužívám výhod vyrovnávání pracovní zátěže klastru.
- Je-li cílový správce front vzdálený a existuje více než jeden kanál, zprávy mohou mít různé přenosové cesty a posloupnost zpráv se stále nezachová.
- Pokud má správce front definici pro přenosovou frontu se stejným názvem jako má správce front místa určení, zprávy se raději nepředávají do přenosové fronty klastru a nikoli v přenosové frontě klastru.

Vrátit název správce front v poli správce front pro odpovědi

Povolit správci front, který obdrží první zprávu v dávce, vrátit její název ve své odpovědi. To provádí pomocí pole ReplyToQMgr deskriptoru zpráv. Správce front na odesílajícím konci pak může extrahovat název správce front odpovědi a zadat jej ve všech následných zprávách.

Použití informací ReplyToQMgr z odezvy má nevýhody:

- Žadající správce front musí čekat na odpověď na svou první zprávu
- Chcete-li vyhledat a použít informace o ReplyToQMgr před odesláním následných zpráv, musíte napsat další kód.
- Pokud existuje více než jedna přenosová cesta ke správci front, pořadí zpráv nemusí být zachováno

Nastavte volbu MQ00_BIND_ON_OPEN u volání MQOPEN .

Vynutíte, aby všechny vaše zprávy byly vloženy do stejného cíle pomocí volby MQ00_BIND_ON_OPEN na volání MQOPEN . Musí být zadán buď MQ00_BIND_ON_OPEN nebo MQ00_BIND_ON_GROUP , když používáte skupiny zpráv s klastry, aby se zajistilo, že všechny zprávy ve skupině budou zpracovány ve stejném cíli.

Otevřením fronty a určením MQ00_BIND_ON_OPEN se vynutí odeslání všech zpráv, které jsou odeslány do této fronty do stejné instance fronty. MQ00_BIND_ON_OPEN váže všechny zprávy ke stejnému správci front a také ke stejné přenosové cestě. Je-li například cesta IP a přenosová cesta NetBIOS ke stejnému místu určení, jeden z nich je vybrán při otevření fronty a tento výběr je poctěn pro všechny zprávy zařazené do stejné fronty pomocí získané popisovače objektu.

Zadáním MQ00_BIND_ON_OPEN vynutíte, aby všechny zprávy byly směrovány do stejného cíle. Aplikace s afinitními zprávami proto nejsou přerušeny. Není-li místo určení k dispozici, zprávy zůstanou v přenosové frontě, dokud nebude znovu k dispozici.

MQ00_BIND_ON_OPEN platí také tehdy, je-li název správce front zadán v deskriptoru objektu při otevření fronty. Jmenovaným správcem front může být více než jedna trasa. Například může existovat více cest k síti nebo jiný správce front může definovat alias. Zadáte-li MQ00_BIND_ON_OPEN, je při otevření fronty vybrána přenosová cesta.

Poznámka: Toto je doporučená technika. Nepracuje však v konfiguraci s více přechody, v níž správce front upozorní na alias pro frontu klastru. Nepomáhá ani v situacích, kdy aplikace používají různé fronty ve stejném správci front pro různé skupiny zpráv.

Alternativou k určení MQ00_BIND_ON_OPEN ve volání MQOPEN je úprava definic front. V definicích front zadejte DEFBIND (OPEN) a povolte volbu DefBind na volání MQOPEN jako standardní nastavení na MQ00_BIND_AS_Q_DEF.

Nastavte volbu MQ00_BIND_ON_GROUP u volání MQOPEN .

Vynutíte, aby všechny zprávy ve skupině byly vloženy do stejného cíle pomocí volby MQ00_BIND_ON_GROUP na volání MQOPEN . Musí být zadán buď MQ00_BIND_ON_OPEN nebo MQ00_BIND_ON_GROUP , když používáte skupiny zpráv s klastry, aby se zajistilo, že všechny zprávy ve skupině budou zpracovány ve stejném cíli.

Otevřením fronty a určením MQ00_BIND_ON_GROUP se vynutí odeslání všech zpráv ve skupině, které jsou odeslány do této fronty, do stejné instance fronty. MQ00_BIND_ON_GROUP váže všechny zprávy ve skupině ke stejnému správci front a také ke stejné přenosové cestě. Pokud například existuje přenosová cesta IP a přenosová cesta NetBIOS do stejného cíle, jeden z nich je vybrán při otevření fronty a tento výběr je poctěn pro všechny zprávy ve skupině zařazené do stejné fronty pomocí získávané popisovače objektu.

Zadáním MQ00_BIND_ON_GROUP vynutíte, aby všechny zprávy ve skupině byly směrovány do stejného cíle. Aplikace s afinitními zprávami proto nejsou přerušeny. Není-li místo určení k dispozici, zprávy zůstanou v přenosové frontě, dokud nebude znovu k dispozici.

MQ00_BIND_ON_GROUP platí také tehdy, je-li název správce front zadán v deskriptoru objektu při otevření fronty. Jmenovaným správcem front může být více než jedna trasa. Například může existovat více cest

k síti nebo jiný správce front může definovat alias. Zadáte-li MQ00_BIND_ON_GROUP, je při otevření fronty vybrána přenosová cesta.

Aby byl produkt MQ00_BIND_ON_GROUP efektivní, musíte zahrnout volbu vložení MQPMO_LOGICAL_ORDER do MQPUT. Můžete nastavit **GroupId** v MQMD zprávy na MQGI_NONE a v poli MQMD **MsgFlags** zprávy musíte zahrnout následující příznaky zpráv:

- Poslední zpráva ve skupině: MQMF_LAST_MSG_IN_GROUP
- Všechny ostatní zprávy ve skupině: MQMF_MSG_IN_GROUP

Je-li zadán parametr MQ00_BIND_ON_GROUP, ale zprávy nejsou seskupeny, chování je ekvivalentní hodnotě MQ00_BIND_NOT_FIXED.

Poznámka: Toto je doporučená metoda pro ujištění, že zprávy ve skupině jsou odeslány do stejného cíle. Nepracuje však v konfiguraci s více přechody, v níž správce front upozorní na alias pro frontu klastru.

Alternativou k určení MQ00_BIND_ON_GROUP ve volání MQOPEN je úprava definic front. V definicích front zadejte DEFBIND(GROUP) a povolte volbu DefBind na volání MQOPEN jako standardní nastavení na MQ00_BIND_AS_Q_DEF.

Napište přizpůsobený výstupní program pracovní zátěže klastru

Místo úpravy aplikací můžete problém s afinitními zprávami obcházet tím, že napíšete uživatelský program pracovní zátěže klastru. Psaní uživatelského programu pracovní zátěže klastru není snadné a není to doporučené řešení. Program by měl být navržen tak, aby rozpoznal afinitu zkoumáním obsahu zpráv. Po rozpoznání afinity by tento program musel vynutit, aby obslužný program správy pracovní zátěže přeměroval všechny související zprávy do stejného správce front.

Konfigurace publikování/odběru zpráv

Můžete spustit, zastavit a zobrazit stav publikování/odběru ve frontě. Můžete také přidávat a odebírat proudy a přidávat a odstraňovat správce front z hierarchie zprostředkovatele.

Další informace o řízení publikací/odběru ve frontě najdete v následujících dílčích tématech:

Nastavení atributů zpráv publikování/odběru ve frontě

Chování některých atributů publikování/odběru atributů můžete řídit pomocí atributů správce front. Další atributy, které budete řídit ve stanze *Broker* souboru *qm.ini*.

Informace o této úloze

Můžete nastavit následující atributy publikování/odběru: podrobnosti viz [Parametry správce front](#).

Popis	Název parametru MQSC
Počet opakování zprávy příkazu	PSRYCNT
Zahodit nedoručitelnou vstupní zprávu příkazu	PSNPMMSG
Chování po nedoručitelné zprávě s odpovědí příkazu	PSNPRES
Zprávy příkazů zpracování v synchronizačním bodě	PSSYNCP

Seke Zprostředkovatel se používá ke správě následujících nastavení konfigurace:

- PersistentPublishRetry=yes | force

Pokud uvedete Yes, pak pokud se nezdaří publikování trvalé zprávy prostřednictvím rozhraní publikování/odběru ve frontě a nebyla požadována žádná záporná odpověď, operace publikování se zopakuje.

Pokud jste si vyžádali negativní odezvu, odešle se negativní odezva a nedojde k dalšímu opakování.

Zadáte-li volbu `Vynutit`, dojde-li k selhání publikování trvalé zprávy prostřednictvím rozhraní publikování/odběru ve frontě, bude operace publikování zopakována, dokud nebude úspěšně zpracována. Neodešle se žádná negativní odezva.

- `NonPersistentPublishRetry= ano | force`

Pokud uvedete `Yes`, pak pokud selže publikování dočasné zprávy prostřednictvím rozhraní publikování/odběru ve frontě, a nebyla požadována žádná negativní odpověď, operace publikování se zopakuje.

Pokud jste si vyžádali negativní odezvu, odešle se negativní odezva a nedojde k dalšímu opakování.

Pokud jste určili volbu `Vynutit`, dojde k selhání publikování netrvalé zprávy prostřednictvím rozhraní publikování/odběru ve frontě, operace publikování bude zopakována, dokud nebude úspěšně zpracována. Neodešle se žádná negativní odezva.

Poznámka: Chcete-li povolit tuto funkci pro netrvalé zprávy a také nastavit hodnotu `NonPersistentPublishRetry`, musíte také zajistit, aby byl atribut správce front `PSSYNCPT` nastaven na hodnotu `Ano`.

Provedení této akce může mít také vliv na výkon dočasných publikování, protože `MQGET` ze fronty `STREAM` se nyní vyskytuje pod synchronizačním bodem.

- `PublishBatchVelikost =číslo`

Zprostředkovatel normálně zpracovává zprávy publikování v rámci synchronizačního bodu. Může být neefektivní potvrdit každou publikaci individuálně, a za určitých okolností může zprostředkovatel zpracovávat více publikovaných zpráv v jediné transakci. Tento parametr určuje maximální počet zpráv publikování, které lze zpracovat v jedné pracovní jednotce.

Výchozí hodnota parametru `PublishBatchSize` je 5.

- `PublishBatchInterval =číslo`

Zprostředkovatel normálně zpracovává zprávy publikování v rámci synchronizačního bodu. Může být neefektivní potvrdit každou publikaci individuálně, a za určitých okolností může zprostředkovatel zpracovávat více publikovaných zpráv v jediné transakci. Tento parametr uvádí maximální dobu (v milisekundách) mezi první zprávou v dávce a jakoukoli následnou publikací zahrnutou do stejné dávky.

Interval dávek 0 označuje, že lze zpracovat až `PublishBatchVelikost` zpráv za předpokladu, že tyto zprávy jsou okamžitě k dispozici.

Výchozí hodnota parametru `PublishBatchInterval` je nula.

Postup

Pomocí Průzkumníka IBM MQ, programovatelných příkazů nebo pomocí příkazu `runmqsc` můžete změnit atributy správce front, které řídí chování publish/odběru.

Příklad

```
ALTER QMGR PSNPRES (SAFE)
```

Spouštění publikování/odběru ve frontě

Než začnete

Přečtěte si popis `PSMODE`, abyste porozuměli třem režimům publikování/odběru:

- `COMPAT`
- `VYPNUTO`
- `POVOLENO`

Informace o této úloze

Nastavte atribut QMGR PSMODE tak, aby se spouštěl buď rozhraní publikování/odběru ve frontě (známé také jako zprostředkovatel), nebo stroj publikování/odběru (také známý jako publish/subscribe verze 7) nebo obojí. Chcete-li zahájit publikování/odběr ve frontě, je třeba nastavit parametr PSMODE na hodnotu ENABLED. Výchozí hodnota je ENABLED.

Postup

Chcete-li povolit rozhraní publikování/odběru ve frontě, je-li rozhraní dosud povoleno, použijte Průzkumníka IBM MQ nebo příkaz `runmqsc`.

Příklad

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

Jak pokračovat dále

Procesy produktu IBM MQ zařazují do fronty příkazy publikování/odběru ve frontě a volání rozhraní MQI (Message Queue Queue Interface) publikování/odběru.

Zastavení publikování/odběru ve frontě

Než začnete

Přečtěte si popis [PSMODE](#), abyste porozuměli třem režimům publikování/odběru:

- COMPAT
- VYPNUTO
- POVOLENO

Informace o této úloze

Nastavte atribut QMGR PSMODE tak, aby se zastavil buď rozhraní publikování/odběru ve frontě (známé také jako zprostředkovatel), nebo stroj publikování/odběru (také známý jako publish/subscribe verze 7) nebo obojí. Chcete-li ukončit publikování/odběr ve frontě, je třeba nastavit parametr PSMODE na hodnotu COMPAT. Chcete-li zcela zastavit stroj publikování/odběru, nastavte PSMODE na DISABLED.

Postup

Chcete-li zakázat rozhraní publikování/odběru ve frontě, použijte Průzkumníka IBM MQ nebo příkaz `runmqsc`.

Příklad

```
ALTER QMGR PSMODE (COMPAT)
```

Přidání proudu

Můžete přidat proudy ručně, abyste povolili izolaci dat mezi aplikacemi, nebo abyste povolili vzájemnou spolupráci s hierarchiemi publikování/odběru Verze 6.

Než začnete

Seznamte se s tím, jak fungují proudy publikování/odběru. Viz [Proudy a témata](#).

Informace o této úloze

K provedení těchto kroků použijte příkaz PCF, `runmqsc` nebo MQ Explorer.

Poznámka: Kroky 1 a 2 můžete provést v libovolném pořadí. Vyplněný krok 3 provedte pouze po dokončení kroků 1 a 2.

Postup

1. Definujte lokální frontu se stejným názvem jako má proud Verze 6 .
2. Definujte lokální téma se stejným názvem jako má proud Verze 6 .
3. Přidejte název fronty do seznamu názvů, SYSTEM.QPUBSUB.QUEUE.NAMELIST
4. Tento postup zopakujte pro všechny správce front verze Verze 7.1 nebo vyšší, kteří jsou v hierarchii publikování/odběru.

přidání 'Sport'

V příkladu sdílení proudů 'Sport', správci front Verze 6 a Verze 7.1 pracují ve stejné hierarchii publikování/odběru. Správci front produktu Verze 6 sdílejí proud s názvem 'Sport'. Příklad ukazuje, jak vytvořit frontu a téma na správci front Verze 7.1 s názvem 'Sport', s řetězcem tématu 'Sport', který je sdílen s proudem Verze 6 'Sport'.

Publikační aplikace Verze 7.1, publikování na téma 'Sport' s řetězcem tématu 'Soccer/Results', vytváří výsledný řetězec tématu 'Sport/Soccer/Results'. Ve správci front produktu Verze 7.1 jsou odběratelé na téma 'Sport' s řetězcem tématu 'Soccer/Results' obdrželi publikování.

Na správci front produktu Verze 6 jsou odběratelé proudu 'Sport' s řetězcem tématu 'Soccer/Results' obdrželi publikování.

```
runmqsc QM1
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM1.
define qlocal('Sport')
  1 : define qlocal('Sport')
AMQ8006: IBM MQ queue created.
define topic('Sport') topicstr('Sport')
  2 : define topic('Sport') topicstr('Sport')
AMQ8690: IBM MQ topic created.
alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport', 'SYSTEM.BROKER.DEFAULT.STREAM',
'SYSTEM.BROKER.ADMIN.STREAM')
  3 : alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport', 'SYSTEM.BROKER.DEFAULT.STREAM',
'SYSTEM.BROKER.ADMIN.STREAM')
AMQ8551: IBM MQ namelist changed.
```

Poznámka: Oba existující názvy v objektu seznamu názvů a nové názvy, které přidáváte do příkazu **alter namelist**, je třeba zadat v názvu objektu seznamu názvů.

Jak pokračovat dále

Informace o proudu se předají ostatním zprostředkovatelům v hierarchii.

Je-li zprostředkovatel Verze 6, spravovat jej jako zprostředkovatele Verze 6 . To znamená, že máte možnost vytvořit frontu proudu ručně, nebo nechat zprostředkovatele dynamicky vytvořit frontu proudu, je-li třeba. Fronta je založena na definici modelové fronty, SYSTEM.BROKER.MODEL.STREAM.

Pokud je zprostředkovatel Verze 7.1, musíte každého správce front Verze 7.1 nakonfigurovat ručně v hierarchii.

Odstranění proudu

Proud můžete odstranit ze správce front produktu IBM MQ Verze 7.1 nebo novější.

Než začnete

Před odstraněním proudu se musíte ujistit, že neexistují žádné zbývající odběry proudu a uvede se do klidového stavu všechny aplikace, které tento proud používají. Pokud publikace pokračují v toku do odstraněného proudu, trvá mnoho administrativních sil k obnově systému do vyčištěného pracovního stavu.

Postup

1. Najít všechny připojené zprostředkovatele, kteří jsou hostiteli tohoto proudu.
2. Zrušit všechny odběry proudu na všech zprostředkovatelů.
3. Odeberte frontu ze seznamu názvů (se stejným názvem jako proud),
SYSTEM.QPUBSUB.QUEUE.NAMELIST.
4. Odstraňte nebo vymažte všechny zprávy z fronty se stejným názvem jako má proud.
5. Odstraňte frontu se stejným názvem, jako má proud.
6. Odstranit přidružený objekt tématu.

Jak pokračovat dále

Zopakujte kroky 3 až 5 ve všech ostatních propojeném produktu Verze 7.1nebo novějším, kteří jsou hostiteli proudu.

Přidání bodu odběru

Jak rozšířit existující aplikaci publikování/odběru ve frontě, kterou jste migrovali ze starší verze produktu IBM Integration Bus s novým bodem odběru.

Než začnete

1. Ověřte, že bod odběru není v produktu SYSTEM.QPUBSUB.SUBPOINT.NAMELISTjiž definován.
2. Zkontrolujte, zda existuje objekt tématu nebo řetězec tématu se stejným názvem jako bod odběru.

Informace o této úloze

Aplikace IBM WebSphere MQ 7.1nebo novější aplikace nepoužívají body odběru, ale mohou spolupracovat s existujícími aplikacemi, které používají mechanismus migrace bodu odběru.

Důležité: Mechanismus migrace bodu odběru byl odebrán z produktu IBM MQ 8.0. Potřebujete-li migrovat existující aplikace, musíte před migrací na nejnovější verzi provést procedury popsané v dokumentaci pro vaši verzi produktu.

Body odběru nepracují s programy publikování/odběru ve frontě, které používají záhlaví produktu MQRFH1 , která byla migrována z produktu IBM MQ verze Verze 6nebo dřívější.

Není třeba přidávat body odběru, které by používaly integrované aplikace publikování/odběru zapsané pro produkt IBM MQ verze Verze 7.1nebo novější.

Postup

1. Přidejte název bodu odběru do produktu SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.
 - V systému z/OSje hodnota **NLTYPE** nastavena na hodnotu NONE(výchozí hodnota).
 - Opakujte tento krok u všech správců front, kteří jsou připojeni ve stejné topologii publikování/odběru.
2. Přidejte objekt tématu, pokud možno jej pojmenujte s názvem bodu odběru, s řetězcem tématu, který odpovídá názvu bodu odběru.
 - Je-li bod odběru umístěn v klastru, přidejte objekt tématu jako téma klastru na hostitele tématu klastru.
 - Pokud objekt tématu existuje se stejným řetězcem tématu jako název bodu odběru, použijte existující objekt tématu. Musíte pochopit důsledky bodu odběru opětovným použitím existujícího tématu. Je-li existující téma součástí existující aplikace, je nutné vyřešit kolizi mezi dvěma identicky pojmenovanými tématy.
 - Existuje-li objekt tématu se stejným názvem jako bod odběru, ale jiný řetězec tématu, vytvořte téma s jiným názvem.
3. Nastavte atribut **Topic WILDCARD** na hodnotu BLOCK.

Zablokování odběrů pro zástupné znaky # nebo * izolují zástupný znak na body odběru, viz [Zástupné znaky a body odběru](#).

4. Nastavte všechny atributy, které vyžadujete v objektu tématu.

Příklad

Tento příklad ukazuje příkazový soubor **runmqsc**, který přidává dva body odběru, USD a GBP.

```
DEFINE TOPIC(USD) TOPICSTR(USD)
DEFINE TOPIC(GBP) TOPICSTR(GBP) WILDCARD(BLOCK)
ALTER NL(SYSTEM.QPUBSUB.SUBPOINT.NAMELIST) NAMES(SYSTEM.BROKER.DEFAULT.SUBPOINT, USD, GBP)
```

Poznámka:

1. Přidejte výchozí bod odběru do seznamu bodů odběru přidáním pomocí příkazu **ALTER**. Příkaz **ALTER** odstraní existující názvy v seznamu názvů.
2. Před změnou seznamu názvů definujte témata. Správce front kontroluje seznam názvů pouze v případě, že je spuštěn správce front a kdy je seznam názvů změněn.

Konfigurace sítě distribuovaných publikování/odběru

Správci front, kteří jsou připojeni k distribuované topologii publikování/odběru, sdílejí společný federovaný prostor tématu. Odběry vytvořené v jednom správci front mohou přijímat zprávy publikované aplikací připojenou k jinému správci front v rámci topologie.

Rozsah prostorů témat vytvořených připojováním správců front v klastrech nebo hierarchiích můžete řídit rozsah vytvořených prostorů témat. V klastru publikování/odběru musí být objekt tématu "klastrovaný" pro každou větev prostoru tématu, který má být rozdělen do klastru. V hierarchii musí být každý správce front nakonfigurován pro identifikaci svého 'nadřazeného' v hierarchii.

Tok publikování a odběrů v rámci topologie můžete dále řídit výběrem toho, zda jsou jednotlivé publikace a odběry buď lokální, nebo globální. Lokální publikování a odběry nejsou šířeny mimo správce front, k němuž je vydavatel nebo odběratel připojen.

Související informace

[Distribuované sítě typu publikování/odběr](#)

[Obor publikování](#)

[Obor odběru](#)

[Prostory tématu](#)

[Definování témat klastru](#)

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER**. Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE**.

Než začnete

Některé konfigurace klastru nemohou pojmout režijní náklady přímého přesměrovaného publikování/odběru. Před použitím této konfigurace prozkoumejte aspekty a volby popsané v tématu [Navrhování klastrů publikování a odběru](#).

Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Viz také [Směrování pro klastry publikování/odběru: Notes on chování](#).

Scénář:

- Klastř INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastřu” na stránce 238. Obsahuje tři správce front; produkty LONDON a NEWYORK obsahují úplná úložiště, produkt PARIS uchovává dílčí úložiště.

Informace o této úloze

Definujete-li téma ve správci front v klastřu, je třeba určit, zda se jedná o téma klastřu, a (je-li tomu tak) směřování v rámci klastřu pro publikování a odběry pro toto téma. Chcete-li provést vytvoření tématu klastřu, nakonfigurujte vlastnost **CLUSTER** na objektu TOPIC s názvem klastřu. Definováním tématu klastřu na správci front v klastřu zpřístupníte téma celému klastřu. Chcete-li zvolit směřování zpráv, které má být použito v klastřu, nastavíte vlastnost **CLROUTE** na objektu TOPIC na jednu z následujících hodnot:

- **DIRECT**
- **TOPICHOST**

Ve výchozím nastavení je směřování témat **DIRECT**. Před produktem IBM MQ 8.0 bylo k dispozici pouze toto směřování. Pokud nakonfigurujete přímo směřované klastřované téma ve správci front, všichni správci front ve klastřu budou mít informace o všech ostatních správcích front ve klastřu. Při provádění operací publikování a odběru se každý správce fronty může připojit přímo k jinému správci fronty v klastřu. Viz téma [Přímé směřované klastřové publikování/odběru](#).

Z produktu IBM MQ 8.0 můžete místo toho konfigurovat směřování témat jako **TOPICHOST**. Při použití směřování hostitelů témat budou mít všichni správci front v klastřu informace o správcích front klastřu, kteří jsou hostiteli směřované definice tématu (tj. správcích front, na kterých jste definovali objekt tématu). Při provádění operací publikování a odběru se správci front v klastřu připojí pouze ke správcům front hostitele tématu a nikoli přímo každý s každým. Správci front hostitele tématu odpovídají za směřování publikování ze správců front, na nichž dochází k publikování publikací, na správce front s odpovídajícími odběry. Viz téma [Klastřové publikování/odběru se směřováním hostitele tématu](#).

Poznámka: Po klastřování objektu tématu (prostřednictvím nastavení vlastnosti **CLUSTER**) nelze změnit hodnotu vlastnosti **CLROUTE**. Před změnou hodnoty musíte vyjmout objekt z klastřu (vlastnost **CLUSTER** nastavit na ' '). Vyřazením tématu z klastřu převedete definici tématu na lokální téma, výsledkem čehož je období, během kterého nebudou publikace doručovány do vzdálených správců front. Tuto skutečnost byste měli při provádění této změny vzít v úvahu. Viz [Dopad definice neklastřového tématu pod názvem tématu klastřu z jiného správce front](#). Pokud se změníte-li se změnit hodnotu vlastnosti **CLROUTE**, zatímco je klastřovaná, vygeneruje systém výjimku MQRCCF_CLROUTE_NOT_ALTERABLE.

Postup

1. Zvolte správce front, který má být hostitelem vašeho tématu.

Kterýkoli správce front klastřu může hostovat téma. Vyberte si jednoho ze tří správců front (LONDON, NEWYORK nebo PARIS) a konfigurujte vlastnosti objektu TOPIC. Plánujete-li používat přímé směřování, nebude již provozní rozdíl mezi vámi a správcem front. Plánujete-li používat směřování hostitelů témat, bude mít vybraný správce front další povinnosti pro směřování publikací. Proto u směřování hostitelů témat zvolte správce front, který je hostován na jednom z vašich výkonnějších systémů a má dobrou síťovou konektivitu.

2. Definujte téma ve správci front.

Chcete-li vytvořit téma klastřu, zahrňte název klastřu při definování tématu a nastavte směřování, které chcete používat pro publikování a odběry pro toto téma. Chcete-li například vytvořit téma klastřu s přímým směřováním ve správci front produktu LONDON, vytvořte následující téma:

```
DEFINE TOPIC(INVENTORY) TOPICSTR('/INVENTORY') CLUSTER(INVENTORY) CLROUTE(DIRECT)
```

Definováním tématu klastřu na správci front v klastřu zpřístupníte téma celému klastřu.

Další informace o použití příkazu **CLROUTE** naleznete v tématu [DEFINE TOPIC \(CLROUTE\)](#) a [Routing pro klastřové publikování/odběru: Notes on chování](#).

Výsledky

Klastr je připraven přijímat publikování a odběry pro dané téma.

Jak pokračovat dále

Pokud jste nakonfigurovali klastr publikování/odběru se směřováním hostitele tématu, pravděpodobně budete chtít pro toto téma přidat další hostitele tématu. Viz [“Přidání dalších hostitelů témat do klastru se směřováním hostitele tématu”](#) na stránce 338.

Pokud máte několik samostatných klastrů publikování/odběru, například protože je vaše organizace geograficky rozptýlená, možná budete chtít rozšířit některá témata klastru do všech klastrů. To můžete provést tak, že propojíte klastry v hierarchii. Viz [“Sloučení prostorů témat u více klastrů”](#) na stránce 344. Můžete také řídit tok publikací z jednoho klastru do jiného. Viz [“Kombinování a izolování prostorů témat ve více klastrech”](#) na stránce 345.

Související pojmy

[Kombinování oborů publikování a odběrů](#)

V produktu IBM MQ verzí 7 a vyšší publikace a obor odběru pracují nezávisle na určení toku publikací mezi správci front.

[Kombinování prostorů témat v sítích typu publikování/odběr](#)

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

[Přesun definice tématu klastru do jiného správce front](#)

Pro klastry routed nebo přímé směřované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

[Přidání dalších hostitelů témat do klastru se směřováním hostitele tématu](#)

V klastru publikování/odběru se směřovaným hostitelem odběru lze více správců front použít k směřování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směřovat přes nového hostitele tématu.

[Připojení správce front k hierarchii publikování a odběru](#)

Podřízený správce front se připojí k nadřízenému správci front v hierarchii. Je-li podřízený správce front již členem jiné hierarchie nebo klastru, spojí toto připojení s hierarchií společně nebo se spojí s klastrem s hierarchií.

[Odpojení správce front z hierarchie publikování/odběru](#)

Odpojit podřízeného správce front z nadřízeného správce front v hierarchii publikování/odběru.

Související informace

[Návrh klastrů publikování a odběru](#)

[Odstraňování problémů distribuovaného publikování/odběru](#)

[Blokující publish/odběr v klastru](#)

Přesun definice tématu klastru do jiného správce front

Pro klastry routed nebo přímé směřované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Informace o této úloze

V klastru můžete mít více definic jednoho objektu tématu klastru. Jedná se o normální stav pro klastr směřování hostitele tématu a neobvyklý stav pro přímo směřovaný klastr. Další informace naleznete v tématu [Několik definic tématu klastru se stejným názvem](#).

Chcete-li přesunout definici tématu klastru do jiného správce front v klastru, aniž byste přerušili tok publikací, postupujte takto. Procedura přesune definici ze správce front QM1 do správce front QM2.

Postup

1. Vytvořte duplikát definice tématu klastru v systému QM2.

Chcete-li směřovat přímé směřování, nastavte všechny atributy tak, aby odpovídaly definici QM1.

V případě směřování hostitele témat nejprve definujte nového hostitele tématu jako PUB (DISABLED). To umožňuje programu QM2 získat informace o odběrech v klastru, ale ne při spouštění směřování publikací.

2. Počkejte, až budou informace šířeny prostřednictvím klastru.

Počkejte, až bude nová definice tématu klastru šířena správci front úplného úložiště do všech správců front v klastru. Použijte příkaz **DISPLAY CLUSTER** k zobrazení témat klastru na každém členu klastru a zkontrolujte definici, která pochází z QM2.

Chcete-li se dozvědět o všech odběrech, počkejte na směřování hostitele témat na nového hostitele tématu QM2. Porovnejte proxy odběry známé pro QM2 a ty, které jsou známé uživateli QM1. Jednou z možností, jak zobrazit proxy odběry ve správci front, je zadání následujícího příkazu **runmqsc** :

```
DISPLAY SUB(*) SUBTYPE(PROXY)
```

3. Pro směřování hostitele témat změňte název hostitele tématu na QM2 jako PUB (ENABLED) a potom předefinujte hostitele témat na QM1 jako PUB (DISABLED).

Nyní, když se nový uzel tématu na systému QM2 dozvěděl o všech odběrech na jiných správcích front, může hostitel tématu zahájit směřování publikací.

Pomocí nastavení PUB (DISABLED) pro uvedení provozu zpráv do klidového stavu pomocí QM1 zajistíte, že žádné publikace nebudou ve vlaku přes QM1, když odstraníte definici tématu klastru.

4. Odstraňte definici tématu klastru z QM1.

Definici můžete odstranit pouze z QM1, je-li správce front k dispozici. Jinak musíte pracovat s oběma definicemi, dokud nebude QM1 restartováno nebo vynuceno odebrání.

Pokud QM1 zůstane nedostupný po dlouhou dobu a během této doby je třeba upravit definici klastrovaného tématu v systému QM2, definice QM2 je novější než definice QM1, a proto obvykle převládne.

Pokud v tomto období existují rozdíly mezi definicemi v systému QM1 a QM2, dojde k zápisu chyb do protokolů chyb obou správců front, které vás upozorní na konfliktní definici tématu klastru.

Pokud se QM1 nikdy nevrátí do klastru, například kvůli neočekávanému vyřazení z provozu po selhání hardwaru, jako poslední možnost můžete použít příkaz **RESET CLUSTER** k vynucenému vysunutí správce front. Příkaz **RESET CLUSTER** automaticky odstraní všechny objekty témat, které jsou hostovány v cílovém správci front.

Související pojmy

Kombinování oborů publikování a odběrů

V produktu IBM MQ verzí 7 a vyšší publikace a obor odběru pracují nezávisle na určení toku publikací mezi správci front.

Kombinování prostorů témat v sítích typu publikování/odběr

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER**.

Chcete-li zvolit směřování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE**.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směřovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování a odběru

Podřízený správce front se připojí k nadřízenému správci front v hierarchii. Je-li podřízený správce front již členem jiné hierarchie nebo klastru, spojí toto připojení s hierarchií společně nebo se spojí s klastrem s hierarchií.

Odpojení správce front z hierarchie publikování/odběru

Odpojit podřízeného správce front z nadřízeného správce front v hierarchii publikování/odběru.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směřovat přes nového hostitele tématu.

Než začnete

Definování stejného objektu tématu klastru v několika správcích front je funkčně užitečné pouze pro klastr se směrováním hostitele tématu. Definování více shodujících se témat v klastru s přímým směrováním nezmění své chování. Tato úloha se týká pouze klastrů se směrováním hostitele tématu.

Tato úloha předpokládá, že jste si přečetli článek Více definic tématu klastru se stejným názvem, a to zejména v následujících sekcích:

- Více definic tématu klastru v klastru se směrováním hostitelů témat
- Speciální zacházení pro parametr PUB

Informace o této úloze

Je-li správce front přesměrován na hostitele témat, musí se nejprve dozvědět o existenci všech souvisejících témat, která jsou přihlášena k odběru v klastru. Pokud jsou publikace publikovány do těchto témat v době, kdy je přidán další hostitel tématu, a publikování je přesměrováno na nového hostitele před tím, než se tento hostitel dozvěděl o existenci odběrů u jiných správců front v klastru, nebude tento nový hostitel přesměrován na tyto odběry. To způsobí, že odběry chybí publikování.

Publikace nejsou směrovány přes správce front hostitele tématu, kteří výslovně nastavili parametr objektu tématu klastru **PUB** na hodnotu **DISABLED**, takže toto nastavení můžete použít k zajištění toho, aby žádné odběry neuniklo během procesu přidávání dalšího hostitele tématu.

Poznámka: Zatímco správce front je hostitelem tématu klastru, které bylo definováno jako **PUB (DISABLED)**, vydavatelé připojené k tomuto správci front nemohou publikovat zprávy a odpovídající odběry v tomto správci front nepřijímají publikování publikovaná v jiných správcích front v klastru. Z tohoto důvodu je třeba pečlivě zvážit definování témat směrována hostitelem tématu u správců front, kde existují odběry a publikování aplikací.

Postup

1. Nakonfigurujte nového hostitele tématu a na počátku definujte nového hostitele tématu jako **PUB (DISABLED)**.

To umožňuje novému hostiteli témat informace o odběrech v klastru, ale ne ke spuštění směrování publikací.

Informace o konfiguraci hostitele témat viz “Konfigurace klastru publikování/odběru” na stránce 334.

2. Určete, kdy se nový hostitel tématu dozvěděl o všech odběrech.

Chcete-li tak učinit, porovnejte proxy odběry známé pro nového hostitele témat a ty, které jsou známy existujícím hostitelům témat. Jednou z možností, jak zobrazit proxy odběry, je vydat následující příkaz **runmqsc** : DISPLAY SUB(*) SUBTYPE (PROXY)

3. Předefinujte nového hostitele tématu jako PUB (ENABLED).

Poté, co se nový uzel tématu dozvěděl o všech odběrech na jiných správcích front, může téma zahájit směrování publikací.

Související pojmy

Kombinování oborů publikování a odběrů

V produktu IBM MQ verzí 7 verzí 7 a vyšší publikace a obor odběru pracují nezávisle na určení toku publikací mezi správci front.

Kombinování prostorů témat v sítích typu publikování/odběr

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesun definice tématu klastru do jiného správce front

Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Připojení správce front k hierarchii publikování a odběru

Podřízený správce front se připojí k nadřizovanému správci front v hierarchii. Je-li podřízený správce front již členem jiné hierarchie nebo klastru, spojí toto připojení s hierarchií společně nebo se spojí s klastrem s hierarchií.

Odpojení správce front z hierarchie publikování/odběru

Odpojit podřízeného správce front z nadřizovaného správce front v hierarchii publikování/odběru.

Kombinování oborů publikování a odběrů

V produktu IBM MQ verzí 7 verzí 7 a vyšší publikace a obor odběru pracují nezávisle na určení toku publikací mezi správci front.

Publikování mohou přejít do všech správců front, kteří jsou připojeni k topologii publikování/odběru nebo pouze lokálnímu správci front. Podobně pro proxy odběry. Informace o tom, které publikace odpovídají odběru, se řídí kombinací těchto dvou toků.

Publikování a odběry mohou mít rozsah hodnot QMGR nebo ALL. Pokud je vydavatel a odběratel připojen ke stejnému správci front, neovlivňují nastavení rozsahu publikování, která odběratel obdrží od tohoto vydavatele.

Pokud je vydavatel a odběratel připojeni k různým správcům front, obě nastavení musí být VŠE , aby bylo možné přijímat vzdálená publikování.

Předpokládejme, že vydavatelé jsou připojeni k různým správcům front. Pokud chcete, aby odběratel přijímal publikování od libovolného vydavatele, nastavte rozsah odběru na hodnotu VŠE. Poté můžete rozhodnout pro každého vydavatele, zda má být omezen rozsah jeho publikací na odběratele lokální pro vydavatele.

Předpokládejme, že odběratelé jsou připojeni k různým správcům front. Pokud chcete, aby byly publikace od vydavatele odeslány všem odběratelům, nastavte rozsah publikování na hodnotu VŠE. Chcete-li odběratele přijímat publikování pouze od vydavatele připojeného ke stejnému správci front, nastavte rozsah odběru na QMGR.

Příklad: služba fotbalových výsledků

Předpokládejme, že jste členský tým ve fotbalové lize. Každý tým má k dispozici správce front připojený ke všem ostatním týmům v klastru publikování/odběru.

Týmy publikují výsledky všech her hraných na jejich domovské zemi pomocí tohoto tématu, `Football/result/Home team name/Away team name`. Řetězce psané kurzívou jsou variabilní názvy témat a publikování je výsledkem shody.

Každý klub také znovu publikuje výsledky pouze pro klub s použitím řetězce tématu `Football/myteam/Home team name/Away team name`.

Obě témata jsou publikována v celém klastru.

Následující odběry byly vytvořeny v lize tak, že fanoušci libovolného týmu se mohou přihlásit k odběru výsledků ve třech zajímavých ohledech.

Všimněte si, že můžete nastavit témata klastru pomocí produktu SUBSCOPE (QMGR). Definice tématu se šíří do každého člena klastru, ale rozsah odběru je pouze lokální správce front. Odběratelé v každém správci front proto obdrží od stejného odběru různé publikace.

Přijmout všechny výsledky

```
DEFINE TOPIC(A) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(ALL)
```

Přijmout všechny domovské výsledky

```
DEFINE TOPIC(B) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR, jsou porovnávány pouze výsledky publikované v domovském umístění.

Přijmout všechny výsledky mých týmů

```
DEFINE TOPIC(C) TOPICSTR('Football/myteam/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR, budou porovnávány pouze lokální výsledky týmu, které se znovu publikují lokálně.

Související pojmy

Kombinování prostorů témat v sítích typu publikování/odběr

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER**. Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE**.

Přesun definice tématu klastru do jiného správce front

Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směřovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování a odběru

Podřízený správce front se připojí k nadřazenému správci front v hierarchii. Je-li podřízený správce front již členem jiné hierarchie nebo klastru, spojí toto připojení s hierarchií společně nebo se spojí s klastrem s hierarchií.

Odpojení správce front z hierarchie publikování/odběru

Odpojit podřízeného správce front z nadřazeného správce front v hierarchii publikování/odběru.

Související informace

Distribuované sítě typu publikování/odběr

Obor publikování

Obor odběru

Kombinování prostorů témat v sítích typu publikování/odběr

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Můžete vytvořit různé prostory tématu pro publikování/odběr pomocí stavebních bloků atributů **CLUSTER**, **PUBSCOPE** a **SUBSCOPE**, klastrů typu publikování/odběr a publikování/odběru hierarchií.

Při spuštění z příkladu změny měřítka z jednoho správce front do klastru publikování/odběru, následující scénáře ilustrují různé topologie publikování/odběru.

Související pojmy

Kombinování oborů publikování a odběrů

V produktu IBM MQ verzí 7 verzí 7 a vyšší publikace a obor odběru pracují nezávisle na určení toku publikací mezi správci front.

Související úlohy

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER**.

Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE**.

Přesun definice tématu klastru do jiného správce front

Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směřovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování a odběru

Podřízený správce front se připojí k nadřazenému správci front v hierarchii. Je-li podřízený správce front již členem jiné hierarchie nebo klastru, spojí toto připojení s hierarchií společně nebo se spojí s klastrem s hierarchií.

Odpojení správce front z hierarchie publikování/odběru

Odpojit podřízeného správce front z nadřazeného správce front v hierarchii publikování/odběru.

Související informace

Distribuované sítě typu publikování/odběr

Prostory tématu

Definování témat klastru

Vytvoření jediného prostoru tématu v klastru publikování/odběru

Rozšířte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

Než začnete

Naimplementovali jste systém typu publikování-odběr u jednoho správce front verze 7.

Vždy vytvářejte prostory tématu s vlastními uživateli root, spíše než spoléháte na dědění atributů produktu SYSTEM . BASE . TOPIC. Pokud škálujete systém publikování/odběru do klastru, můžete definovat kořenové témata jako témata klastru, na hostiteli témat klastru a poté všechny vaše témata sdílet v rámci celého klastru.

Informace o této úloze

Nyní chcete rozšířit systém tak, aby podporoval více vydavatelů a odběratelů a aby měl každé téma viditelné v rámci celého klastru.

Postup

1. Vytvořte klastr, který má být použit se systémem publikování/odběru.
Máte-li existující tradiční klastr, z důvodu výkonu je lepší nastavit nový klastr pro nový systém odběru publikování. Pro úložiště klastru u obou klastrů můžete použít stejné servery.
2. Vyberte jednoho správce front, pravděpodobně jednoho z úložišť, který bude hostitelem tématu klastru.
3. Ujistěte se, že každé téma, které má být viditelné v rámci klastru publikování/odběru, se interpretuje jako objekt tématu administrace.
Nastavte atribut **CLUSTER** pro pojmenování klastru publikování/odběru.

Jak pokračovat dále

Připojte vydavatele a aplikace odběratele do všech správců front v klastru.

Vytvořte objekty administrativního tématu, které mají atribut **CLUSTER**. Témata se také šíří do celého klastru. Programy vydavatele a odběratele používají administrativní témata, aby jejich chování nebylo změněno tím, že je připojeno k různým správcům front v klastru.

Pokud potřebujete produkt SYSTEM . BASE . TOPIC v každém správci front vystupovat jako téma klastru, je třeba jej upravit ve všech správcích front.

Související úlohy

Přidání správce front verze 7 nebo novější do existujících prostorů témat Verze 6

Rozšířte existující systém publikování/odběru produktu Verze 6 tak, aby pracoval se správcem front verze 7 nebo novější a sdílel stejné prostory témat.

Sloučení prostorů témat u více klastrů

Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Kombinování a izolování prostorů témat ve více klastrech

Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

Publikování a přihlášení k odběru prostorů témat ve více klastrech

Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Související informace

Distribuované síť typu publikování/odběr

Prostory tématu

Definování témat klastru

Přidání správce front verze 7 nebo novější do existujících prostorů témat Verze 6

Rozšířte existující systém publikování/odběru produktu Verze 6 tak, aby pracoval se správcem front verze 7 nebo novější a sdílel stejné prostory témat.

Než začnete

You have an existing Verze 6 publish/subscribe system.

Nainstalovali jste produkt IBM MQ verze 7 nebo novější na nový server a nakonfigurovali jste správce front.

Informace o této úloze

Chcete rozšířit existující systém publikování/odběru Verze 6 tak, aby pracoval s správcí front verze 7 nebo novější.

Rozhodli jste se stabilizovat vývoj systému publikování/odběru Verze 6, který používá rozhraní publikování/odběru ve frontě. Zamýšlíte přidat rozšíření do systému pomocí rozhraní MQI verze 7 nebo novější. Nyní nemáte žádné plány na přepsání aplikací publikování/odběru ve frontě.

Plánujete upgradovat správce front produktu Verze 6 na verzi 7 nebo novější v budoucnu. Prozatím nadále spouštíte existující aplikace publikování/odběru ve frontě ve správcí front verze 7 nebo vyšší.

Postup

1. Vytvořte jednu sadu přijímacích kanálů odesílatele pro připojení správce front verze 7 nebo novější k jednomu ze správců front produktu Verze 6 v obou směrech.
2. Vytvořte dvě přenosové fronty s názvy cílových správců front. Alias správce front použijte, pokud z nějakého důvodu nelze použít název cílového správce front jako název přenosové fronty.
3. Konfigurujte přenosové fronty tak, aby spustily odesílací kanály.
4. Pokud systém publikování/odběru Verze 6 používá proudy, přidejte proudy do správce front verze 7 nebo novější, jak je popsáno v tématu [Přidání proudu](#).
5. Zkontrolujte, zda je správce front verze 7 nebo novější **PSMODE** nastaven na hodnotu ENABLE.
6. Změňte její atribut **PARENT** tak, aby odkazoval na jednoho ze správců front produktu Verze 6.
7. Zkontrolujte, zda je stav relace nadřazený-podřazený mezi správcí front aktivní v obou směrech.

Jak pokračovat dále

Po dokončení úlohy sdílí správce front produktu Verze 6 i správce front verze 7 nebo novější stejné prostory témat. Můžete například provést všechny následující úlohy.

- Vyměňujte publikace a odběry mezi správcí front Verze 6 a verze 7 nebo novější.
- Spusťte existující programy publikování/odběru Verze 6 ve správcí front verze 7 nebo vyšší.
- Zobrazte a upravte prostor tématu buď ve správcí front Verze 6, nebo v produktu verze 7 nebo novějším.
- Zapisovat/odebírat aplikace verze 7 nebo novější a spouštět je ve správcí front verze 7 nebo vyšší.
- Vytvářejte nové publikace a odběry s aplikacemi verze 7 nebo novější a vyměňujete je s aplikacemi produktu Verze 6.

Související úlohy

[Vytvoření jediného prostoru tématu v klastru publikování/odběru](#)

Rozšířte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

[Sloučení prostorů témat u více klastrů](#)

Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

[Kombinování a izolování prostorů témat ve více klastrech](#)

Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

[Publikování a přihlášení k odběru prostorů témat ve více klastrech](#)

Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Související informace

[Distribuované sítě typu publikování/odběr](#)

[Prostory tématu](#)

[Definování témat klastru](#)

Sloučení prostorů témat u více klastrů

Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Než začnete

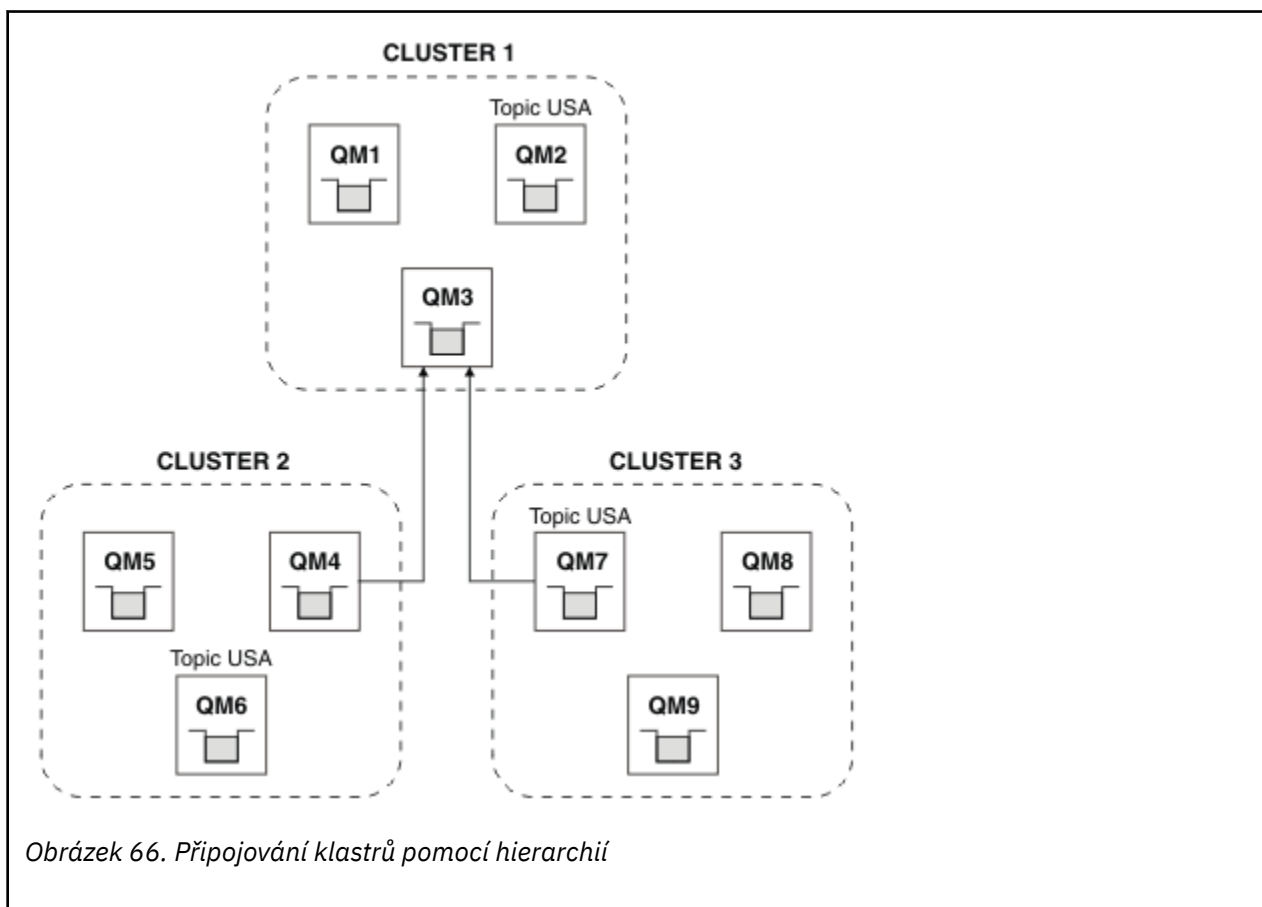
Tato úloha předpokládá, že máte existující přímo směřované klastry publikování/odběru, a chcete šířit některá témata klastru do všech klastrů.

Poznámka: To nelze provést pro klastry publikování/odběru se směřováním hostitelů/odběru.

Informace o této úloze

Chcete-li šířit publikace z jednoho klastru do jiného, musíte se připojit ke klastrům společně v hierarchii; viz [Obrázek 66 na stránce 344](#). Hierarchická připojení šíří odběry a publikování mezi propojenými správci front a klastry šíří témata klastru v rámci jednotlivých klastrů, ale nikoli mezi klastry.

Kombinace těchto dvou mechanismů šíří témata klastru mezi všemi klastry. Je třeba, abyste v každém klastru zopakovali definice tématu klastru.



Obrázek 66. Připojování klastrů pomocí hierarchií

Následující kroky spojují klastry do hierarchie.

Postup

1. Vytvořte dvě sady přijímacích kanálů odesílatele k připojení produktů QM3 a QM4a QM3 a QM7v obou směrech. Chcete-li připojit hierarchii, musíte použít tradiční odesílací kanály odesílatele a přenosové fronty, spíše než klastr.
2. Vytvořte tři přenosové fronty s názvy cílových správců front. Alias správce front použijte, pokud z nějakého důvodu nelze použít název cílového správce front jako název přenosové fronty.
3. Konfigurujte přenosové fronty tak, aby spustily odesílací kanály.
4. Zkontrolujte, zda je **PSMODE** z QM3, QM4 a QM7 nastaveno na ENABLE.
5. Pozměňte atribut **PARENT** z QM4 a QM7 na QM3.
6. Zkontrolujte, zda je stav relace nadřazený-podřazený mezi správcí front aktivní v obou směrech.
7. Vytvořte administrativní téma USA s atributem **CLUSTER** (' CLUSTER 1 '), **CLUSTER** (' CLUSTER 2 ') a **CLUSTER** (' CLUSTER 3 ') na každém ze tří správců front hostitele tématu klastru v klastrech 1, 2 a 3. Hostitele tématu klastru nemusí být hierarchicky připojeným správcem front.

Jak pokračovat dále

Nyní můžete publikovat nebo přihlásit se k odběru tématu klastru USA v produktu [Obrázek 66 na stránce 344](#). Publikování odběrů publikování pro vydavatele a odběratele ve všech třech klastrech.

Předpokládejme, že jste nevytvořili USA jako téma klastru v ostatních klastrech. Je-li USA definováno pouze v systému QM7, jsou publikace a odběry USA vyměňovány mezi QM7, QM8, QM9a QM3. Vydavatelé a odběratelé spuštění v systému QM7, QM8, QM9 dědí atributy administrativního tématu USA. Vydavatelé a odběratelé na QM3 dědí atributy z SYSTEM . BASE . TOPIC na QM3.

Další informace najdete v tématu [“Kombinování a izolování prostorů témat ve více klastrech” na stránce 345](#).

Související úlohy

[Vytvoření jediného prostoru tématu v klastru publikování/odběru](#)

Rozšířte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

[Přidání správce front verze 7 nebo novější do existujících prostorů témat Verze 6](#)

Rozšířte existující systém publikování/odběru produktu Verze 6 tak, aby pracoval se správcem front verze 7 nebo novější a sdílel stejné prostory témat.

[Kombinování a izolování prostorů témat ve více klastrech](#)

Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

[Publikování a přihlášení k odběru prostorů témat ve více klastrech](#)

Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Související informace

[Distribuované sítě typu publikování/odběr](#)

[Prostory tématu](#)

[Definování témat klastru](#)

Kombinování a izolování prostorů témat ve více klastrech

Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

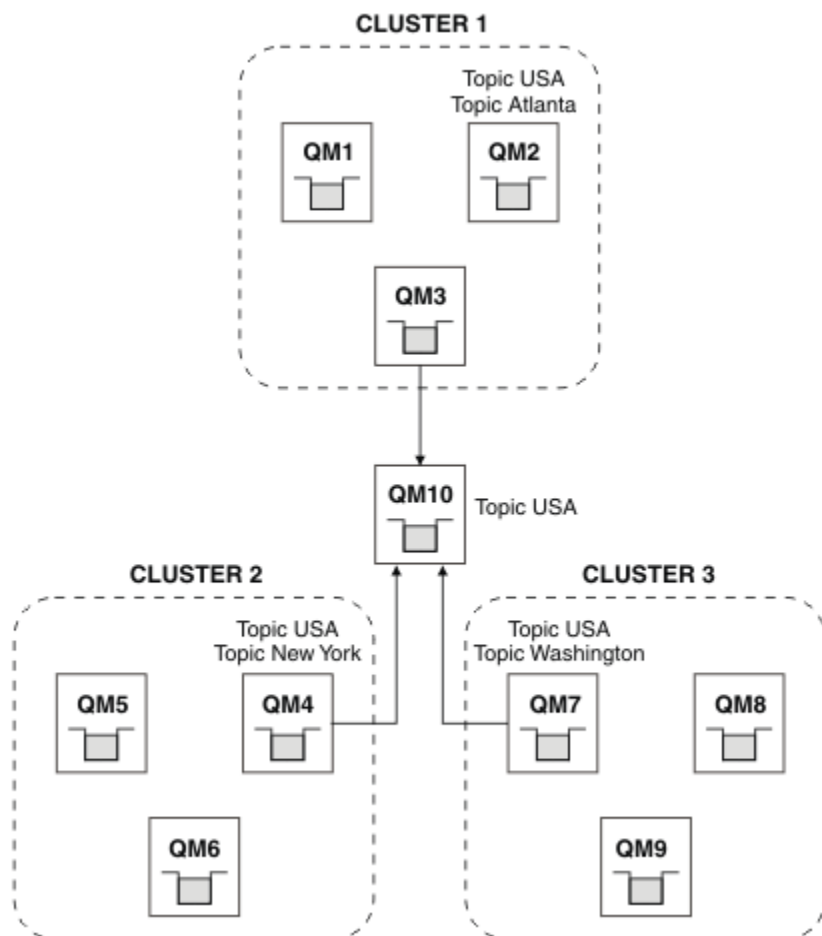
Než začnete

Proveďte téma [“Sloučení prostorů témat u více klastrů” na stránce 344](#). Může to být dostačující pro vaše potřeby, aniž byste přidali dalšího správce front jako most.

Poznámka: Tuto úlohu lze provést pouze pomocí přímých směrovaných klastrů publikování/odběru. To nelze provést pomocí klastrů se směrováním hostitele tématu.

Informace o této úloze

Potenciální zlepšení topologie zobrazené v produktu Obrázek 66 na stránce 344 v produktu “Sloučení prostorů témat u více klastrů” na stránce 344 spočívá v izolaci témat klastru, která nejsou sdílena mezi všemi klastry. Izolovat klastry vytvořením přemosťovacího správce front, který není v žádném z klastrů; viz Obrázek 67 na stránce 346. Pomocí správce front pro přemostění můžete filtrovat, které publikace a odběry mohou přecházet z jednoho klastru do jiného.



Obrázek 67. Propojené klastry

Pomocí mostu určete témata klastru, která nechcete vystavit na základě mostu na ostatních klastrech. V produktu Obrázek 67 na stránce 346 je USA téma klastru sdílené ve všech klastrech a produkty Atlanta, New York a Washington jsou témata klastru, která jsou sdílena pouze v jednom klastru.

Modelujte konfiguraci pomocí následující procedury:

Postup

1. Upravte všechny objekty tématu produktu SYSTEM.BASE.TOPIC tak, aby měly produkt **SUBSCOPE** (QMGR). a **PUBSCOPE** (QMGR) na všech správcích front.
Žádná témata (ani témata klastru) se nešíří do jiných správců front, pokud jste explicitně nenastavovali **SUBSCOPE** (ALL). a **PUBSCOPE** (ALL) v tématu týkajícím se kořenového adresáře témat klastru.
2. Definujte témata na třech správcích front hostitele témat klastru, které chcete sdílet v každém klastru s atributy **CLUSTER** (*clustername*), **SUBSCOPE** (ALL). a **PUBSCOPE** (ALL).
Chcete-li některá témata klastru sdílet mezi všemi klastry, definujte stejné téma v každém z klastrů. Jako atribut klastru použijte název klastru každého klastru.
3. V případě témat klastru, která chcete sdílet mezi všemi klastry, definujte témata znovu ve správcích front mostu (QM10) s atributy **SUBSCOPE** (ALL) a **PUBSCOPE** (ALL).

Příklad

V příkladu v produktu [Obrázek 67](#) na stránce 346 se šíří pouze témata, která dědí od USA mezi všemi třemi klastry.

Jak pokračovat dále

Odběry pro témata definovaná ve správci front mostu s produktem **SUBSCOPE** (ALL) a **PUBSCOPE** (ALL) jsou šířeny mezi klastry.

Odběry pro témata definovaná v rámci každého klastru s atributy **CLUSTER** (*clustername*), **SUBSCOPE** (ALL) a **PUBSCOPE** (ALL) jsou šířeny v rámci každého klastru.

Všechny ostatní odběry jsou lokální pro správce front.

Související úlohy

[Vytvoření jediného prostoru tématu v klastru publikování/odběru](#)

Rozšířte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

[Přidání správce front verze 7 nebo novější do existujících prostorů témat Verze 6](#)

Rozšířte existující systém publikování/odběru produktu Verze 6 tak, aby pracoval se správcem front verze 7 nebo novější a sdílel stejné prostory témat.

[Sloučení prostorů témat u více klastrů](#)

Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

[Publikování a přihlášení k odběru prostorů témat ve více klastrech](#)

Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Související informace

[Distribuované sítě typu publikování/odběr](#)

[Prostory tématu](#)

[Definování témat klastru](#)

[Obor publikování](#)

[Obor odběru](#)

Publikování a přihlášení k odběru prostorů témat ve více klastrech

Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Než začnete

Vytvořte více tradičních klastrů s některými správci front v průsečících mezi klastry.

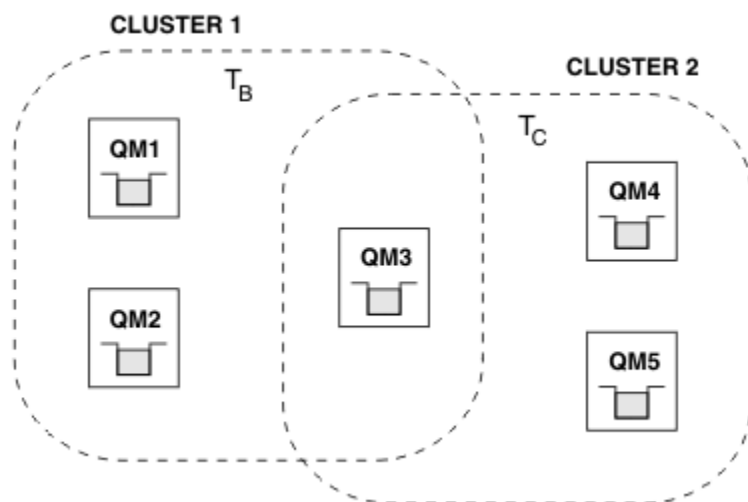
Informace o této úloze

Možná jste se rozhodli překrývat klastry pro různé různé důvody.

1. Máte omezený počet serverů s vysokou dostupností nebo správců front. Rozhodli jste se implementovat všechna úložiště klastru a hostitele klastru k nim.
2. Máte existující klastry tradičních správců front, které jsou připojeny pomocí správců front brány. Chcete implementovat aplikace publikování/odběru do stejné topologie klastru.
3. Máte několik samostatně obsažených aplikací typu publikování/odběr. Z výkonnostních důvodů je lepší udržovat malé a oddělené klastry publikování/odběru odděleně od tradičních klastrů. Rozhodli jste se implementovat aplikace do různých klastrů. Avšak také chcete monitorovat všechny aplikace publikování/odběru na jednom správci front, protože jste licencovali pouze jednu kopii aplikace monitorování. Tento správce front musí mít přístup k publikacím na témata klastru ve všech klastrech.

Tím, že zajistíte, aby vaše témata byla definována v nepřekrývaných prostorech témat, můžete implementovat témata do překrývajících se klastrů publikování/odběru, viz [Obrázek 68](#) na stránce 348. Pokud se mezery tématu překrývají, pak implementace do překrývajících se klastrů bude mít za následek problémy.

Vzhledem k tomu, že klastry publikování/odběru se překrývají, můžete publikovat a odebírat kterýkoli z prostorů témat používajících správce front v překryvu.



Obrázek 68. Překrývající se klastry, nepřekrývající se prostory tématu

Postup

Vytvořte prostředek, který zajistí, aby se prostory tématu nepřekrývaly.

Například definujte jedinečné kořenové téma pro každý z prostorů témat. Témata týkající se klastru kořenových témat proveďte jako témata.

- a) DEFINE TOPIC(B) TOPICSTR('B') CLUSTER('CLUSTER 1') ...
- b) DEFINE TOPIC(C) TOPICSTR('C') CLUSTER('CLUSTER 2') ...

Příklad

V produktu [Obrázek 68](#) na stránce 348 vydavatelé a odběratel, který je připojen k produktu QM3, může publikovat nebo odebírat T_B nebo T_C

Jak pokračovat dále

Navázat vydavatele a odběratele, kteří používají témata v obou klastrech pro správce front v překryvu.

Připojte vydavatele a odběratele, kteří musí používat pouze témata ve specifickém klastru pro správce front, kteří nejsou v překryvu.

Související úlohy

[Vytvoření jediného prostoru tématu v klastru publikování/odběru](#)

Rozšířte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klaster publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

[Přidání správce front verze 7 nebo novější do existujících prostorů témat Verze 6](#)

Rozšířte existující systém publikování/odběru produktu Verze 6 tak, aby pracoval se správcem front verze 7 nebo novější a sdílel stejné prostory témat.

[Sloučení prostorů témat u více klastrů](#)

Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Kombinování a izolování prostorů témat ve více klastrech

Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

Související informace

Distribuované sítě typu publikování/odběr

Prostory tématu

Definování témat klastru

Připojení správce front k hierarchii publikování a odběru

Podřízený správce front se připojí k nadřízenému správci front v hierarchii. Je-li podřízený správce front již členem jiné hierarchie nebo klastru, spojí toto připojení s hierarchií společně nebo se spojí s klastrem s hierarchií.

Než začnete

1. Správci front v hierarchii publikování/odběru musí mít jedinečné názvy správců front.
2. Hierarchie publikování/odběru spoléhá na funkci správce front "publikování/odběru ve frontě" . Tato akce musí být povolena jak pro nadřízené, tak i pro podřízené správce front. Další informace naleznete v tématu Spuštění publikování a odběru ve frontě.
3. Vztah publikování a odběru spoléhá na odesílací kanály správce front a kanály příjemce. K dispozici jsou dva způsoby vytvoření kanálů:
 - Přidejte nadřízený a podřízený správce front do klastru IBM MQ . Viz Přidání správce front do klastru.
 - Vytvořte dvojici odesílatel/příjemce kanálu z podřízeného správce front do nadřízeného a z nadřízeného do podřízeného správce front. Každý kanál buď potřebuje použít přenosovou frontu se stejným názvem jako je cílový správce front, nebo alias správce front se stejným názvem jako má cílový správce front. Další informace o tom, jak zavést dvoubodové připojení kanálu, najdete v tématu IBM MQ technologie distribuovaných front.

Příklady konfigurace hierarchie pro jednotlivé typy konfigurace kanálů naleznete v následující sadě scénářů hierarchie publikování/odběru:

- Scénář 1: Použití dvoubodových kanálů s aliasem názvu správce front
- Scénář 2: Použití dvoubodových kanálů se stejným názvem pro přenosovou frontu a vzdáleného správce front
- Scénář 3: Použití kanálu klastru pro přidání správce front

Informace o této úloze

Použijte příkaz `ALTER QMGR PARENT (PARENT_NAME) runmqsc` k připojení podřízených prvků k nadřazeným prvkům. Tato konfigurace se provádí na podřízeném správci front, kde `PARENT_NAME` je název nadřízeného správce front.

Postup

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

Příklad

První příklad ukazuje, jak připojit správce front QM2 jako podřízený prvek QM1, poté se dotázat QM2 na potvrzení, že se úspěšně stal podřízeným prvkem s **STATUS ACTIVE**:

```
C:>runmqsc QM2
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM2
alter qmgr parent(QM1)
1 : alter qmgr parent(QM1)
```

```

AMQ8005: IBM MQ queue manager changed.
display pubsub all
  2 : display pubsub all
AMQ8723: Display pub/sub status details.
      QMNAME(QM2)                TYPE(LOCAL)
      STATUS(ACTIVE)
AMQ8723: Display pub/sub status details.
      QMNAME(QM1)                TYPE(PARENT)
      STATUS(ACTIVE)

```

Další příklad ukazuje výsledek dotazu QM1 pro svá připojení:

```

C:\Documents and Settings\Admin>runmqsc QM1
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM1.
display pubsub all
  2 : display pubsub all
AMQ8723: Display pub/sub status details.
      QMNAME(QM1)                TYPE(LOCAL)
      STATUS(ACTIVE)
AMQ8723: Display pub/sub status details.
      QMNAME(QM2)                TYPE(CHILD)
      STATUS(ACTIVE)

```

Pokud se **STATUS** nezobrazuje jako AKTIVNÍ, zkontrolujte, zda jsou kanály mezi podřízeným a nadřízeným prvkem správně nakonfigurovány a spuštěny. Zkontrolujte, zda v protokolech chyb správce front nejsou možné chyby.

Jak pokračovat dále

Ve výchozím nastavení jsou témata používaná vydavateli a odběrateli v jednom správci front sdílena s vydavateli a odběrateli na ostatních správčích front v hierarchii. Spravované témata lze nakonfigurovat tak, aby bylo možné kontrolovat úroveň sdílení prostřednictvím použití vlastností témat **SUBSCOPE** a **PUBSCOPE**. Viz téma [Konfigurace distribuovaných sítí pro publikování/odběr](#).

Související pojmy

[Kombinování oborů publikování a odběrů](#)

V produktu IBM MQ verzí 7 a vyšší publikace a obor odběru pracují nezávisle na určení toku publikací mezi správci front.

[Kombinování prostorů témat v sítích typu publikování/odběr](#)

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

[Konfigurace klastru publikování/odběru](#)

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER**. Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE**.

[Přesun definice tématu klastru do jiného správce front](#)

Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

[Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu](#)

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směřovat přes nového hostitele tématu.

[Odpojení správce front z hierarchie publikování/odběru](#)

Odpojit podřízeného správce front z nadřízeného správce front v hierarchii publikování/odběru.

Související informace

[Proudy a témata](#)

Odpojení správce front z hierarchie publikování/odběru

Odpojit podřízeného správce front z nadřízeného správce front v hierarchii publikování/odběru.

Informace o této úloze

K odpojení správce front z hierarchie zprostředkovatele použijte příkaz **ALTER QMGR**. Správce front můžete kdykoli odpojit v libovolném pořadí.

Odpovídající požadavek na aktualizaci nadřazené položky se odešle, když je spuštěno připojení mezi správcem front.

Postup

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

Příklad

```
C:\Documents and Settings\Admin>runmqsc QM2
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM2.
  1 : alter qmgr parent('')
AMQ8005: IBM MQ queue manager changed.
  2 : display pubsub type(child)
AMQ8147: IBM MQ object not found.
display pubsub type(parent)
  3 : display pubsub type(parent)
AMQ8147: IBM MQ object not found.
```

Jak pokračovat dále

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

Související pojmy

[Kombinování oborů publikování a odběrů](#)

V produktu IBM MQ verzí 7 a vyšší publikace a obor odběru pracují nezávisle na určení toku publikací mezi správcem front.

[Kombinování prostorů témat v sítích typu publikování/odběr](#)

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

[Konfigurace klastru publikování/odběru](#)

Definujte téma ve správcem front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER**.

Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLRROUTE**.

[Přesun definice tématu klastru do jiného správce front](#)

Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

[Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu](#)

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směřovat přes nového hostitele tématu.

[Připojení správce front k hierarchii publikování a odběru](#)

Podřízený správce front se připojí k nadřízenému správci front v hierarchii. Je-li podřízený správce front již členem jiné hierarchie nebo klastru, spojí toto připojení s hierarchií společně nebo se spojí s klastrem s hierarchií.

Konfigurace více instalací

Používáte-li více instalací ve stejném systému, musíte nakonfigurovat instalace a správce front.

Tyto informace platí pro SYSTÉM UNIX, Linuxa Okna.

Při konfiguraci vašich instalací použijte informace v následujících odkazech:

- [“Změna primární instalace” na stránce 360](#)
- [“Přidružení správce front k instalaci” na stránce 362](#)
- [“Připojování aplikací v prostředí s více instalačními prostředí” na stránce 352](#)

Související informace

[Výběr primární instalace](#)

[Více instalací](#)

[Výběr názvu instalace](#)

Připojování aplikací v prostředí s více instalačními prostředí

On SYSTÉM UNIX, Linuxa Okna systems, if IBM WebSphere MQ 7.1, or later, libraries are loaded, IBM MQ automatically uses the appropriate libraries without you needing to take any further action. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Následující koncepty se používají k vysvětlení způsobu připojení aplikací k produktu IBM MQ:

propojení

Při kompilování aplikace je aplikace propojena s knihovnami produktu IBM MQ , aby získal export funkcí, který se poté načte při spuštění aplikace.

Zavádění

Když je aplikace spuštěna, jsou umístěny a zavedeny knihovny produktu IBM MQ . Specifický mechanismus použitý k vyhledání knihoven se liší podle operačního systému a podle toho, jak je aplikace sestavena. Další informace o tom, jak vyhledat a načíst knihovny ve více instalačních prostředích, najdete v tématu [“Načtení produktu IBM WebSphere MQ 7.1nebo novější verze knihoven”](#) na stránce 354.

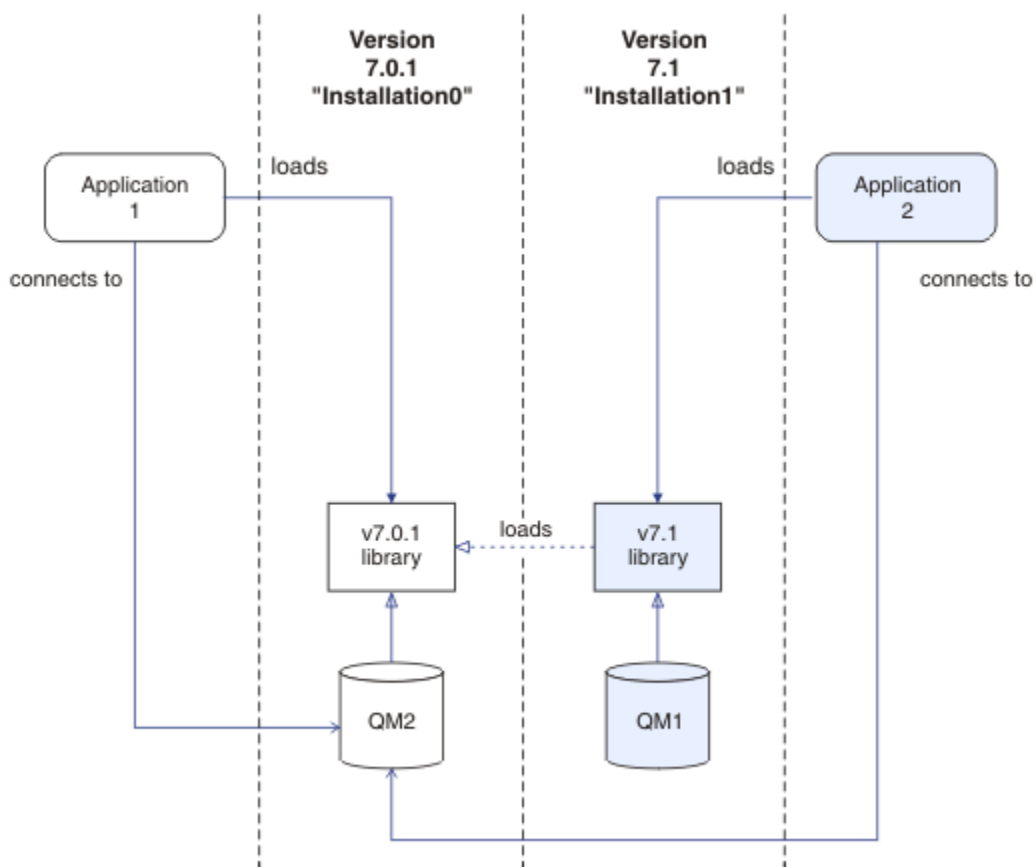
Připojování

Když se aplikace připojí ke spuštěnému správci front, například pomocí volání MQCONN nebo MQCONNX , připojí se k použití načtených knihoven produktu IBM MQ .

Když se serverová aplikace připojuje ke správci front, musí načtené knihovny pocházet z instalace přidružené ke správci front. Při použití více instalací v systému toto omezení představuje nové problémy při výběru mechanismu, který operační systém používá k vyhledání knihoven produktu IBM MQ , které mají být načteny:

- Pokud se příkaz **setmqm** používá ke změně instalace přidružené ke správci front, knihovny, které je třeba načíst, se mění.
- Když se aplikace připojuje k více správcům front, kteří jsou vlastněny různými instalacemi, musí být načteno více sad knihoven.

Nicméně, pokud je IBM WebSphere MQ 7.1nebo pozdější knihovny, jsou umístěny a zavedeny, IBM MQ pak zavede a použije příslušné knihovny, aniž byste potřebovali provést další akce. Když se aplikace připojí ke správci front, produkt IBM MQ načte knihovny z instalace, ke které je přidružen správce front.



Obrázek 69. Připojování aplikací v prostředí s více instalačními prostředí

Například Obrázek 69 na stránce 353 ukazuje vícenásobné instalační prostředí s instalací produktu Verze 7.0.1 (Installation0) a instalací produktu Verze 7.1 (Installation1). K těmto instalacím jsou připojeny dvě aplikace, ale načítají různé verze knihoven.

Produkt Application 1 přímo načte knihovnu Verze 7.0.1 . Když se produkt application 1 připojí k produktu QM2, použijí se knihovny Verze 7.0.1 . Pokud se produkt application 1 pokusí o připojení k produktu QM1nebo pokud je QM2 přidružen k produktu Installation1, dojde k selhání application 1 s chybou 2059 (080B) (RC2059): MQRC_Q_MGR_NOT_AVAILABLE . Aplikace selže, protože knihovna Verze 7.0.1 není schopna načíst jiné verze knihovny. To znamená, že pokud jsou knihovny Verze 7.0.1 přímo načteny, nelze k instalaci použít správce front přidruženého k instalaci v novější verzi produktu IBM MQ.

Produkt Application 2 přímo načte knihovnu Verze 7.1 . Když se produkt application 2 připojí k produktu QM2, knihovna Verze 7.1 se pak načte a použije knihovnu Verze 7.0.1 . Pokud se produkt application 2 připojí k produktu QM1nebo pokud je QM2 přidružen k produktu Installation1, je načtena knihovna Verze 7.1 a aplikace pracuje podle očekávání.

Scénáře migrace a připojení aplikací s více instalacemi jsou podrobněji zváženy v tématu Koexistence více instalačních správců front v produktu SYSTÉM UNIX, Linuxa Okna .

Další informace o způsobu načítání knihoven produktu IBM WebSphere MQ 7.1 naleznete v tématu “Načtení produktu IBM WebSphere MQ 7.1nebo novější verze knihoven” na stránce 354.

Podpora a omezení

Pokud jsou umístěny a načteny některé z následujících knihoven Verze 7.1nebo novější, může produkt IBM MQ automaticky načíst a použít příslušné knihovny:

- Knihovny serveru jazyka C

- Knihovny serveru C++
- Knihovny serveru XA
- Knihovny serveru COBOL
- Knihovny serveru COM +
- .NET v nespravovaném režimu

Produkt IBM MQ také automaticky načítá a používá příslušné knihovny pro aplikace Java a JMS v režimu vazeb.

Pro aplikace používající více instalací existuje několik omezení. Další informace viz [“Omezení pro aplikace používající více instalací”](#) na stránce 357.

Související pojmy

[“Přidružení správce front k instalaci”](#) na stránce 362

Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz `crtmqm`. V systému SYSTÉM UNIX, Linuxu Oknamůžete změnit instalaci přidruženou ke správci front pomocí příkazu `setmqm`.

[“Omezení pro aplikace používající více instalací”](#) na stránce 357

Existují omezení při použití knihoven serveru produktu CICS, připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními podmínkami.

[“Načtení produktu IBM WebSphere MQ 7.1nebo novější verze knihoven”](#) na stránce 354

Při rozhodování o načtení knihoven produktu IBM MQ je třeba zvážit řadu faktorů, včetně: vašeho prostředí, zda můžete změnit existující aplikace, zda chcete primární instalaci, kde je nainstalován produkt IBM MQ a zda se bude umístění produktu IBM MQ pravděpodobně měnit.

Související úlohy

[“Změna primární instalace”](#) na stránce 360

K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz `setmqinst`.

Související informace

[Výběr primární instalace](#)

Načtení produktu IBM WebSphere MQ 7.1nebo novější verze knihoven

Při rozhodování o načtení knihoven produktu IBM MQ je třeba zvážit řadu faktorů, včetně: vašeho prostředí, zda můžete změnit existující aplikace, zda chcete primární instalaci, kde je nainstalován produkt IBM MQ a zda se bude umístění produktu IBM MQ pravděpodobně měnit.

Jak produkt IBM WebSphere MQ 7.1, nebo pozdější verze knihoven jsou umístěny a načteny závisí na vašem prostředí instalace:

- Je-li v systému SYSTÉM UNIX a Linux nainstalována kopie produktu IBM WebSphere MQ 7.1nebo novější verze ve výchozím umístění, stávající aplikace budou nadále pracovat stejným způsobem jako předchozí verze. Pokud však aplikace potřebují symbolické odkazy v produktu `/usr/lib`, musíte buď vybrat instalaci produktu Verze 7.1nebo pozdější verzi, instalaci jako primární instalaci, nebo ručně vytvořit symbolické odkazy.
- Je-li produkt IBM WebSphere MQ 7.1nebo novější verze nainstalován v jiném než výchozím umístění, což je případ, kdy je nainstalován také produkt IBM WebSphere MQ 7.0.1, může být zapotřebí změnit existující aplikace tak, aby byly načteny správné knihovny.

Jak produkt IBM WebSphere MQ 7.1, nebo pozdější verze, knihovny lze vyhledat a načíst také závisí na tom, jak jsou všechny existující aplikace nastaveny na zaváděcí knihovny. Další informace o tom, jak lze načíst knihovny, najdete v tématu [“Mechanismy zavádění knihoven operačního systému”](#) na stránce 356.

Optimálně byste měli zajistit, aby knihovna IBM MQ, která je zavedena operačním systémem, byla přidružena k tomuto správci front.

Metody načítání knihoven IBM MQ se liší podle platformy a každá z těchto metod má výhody a nevýhody.

Tabulka 27. Výhody a nevýhody voleb pro načítání knihoven

Platforma	Volba	Výhody	Nevýhody
<p>Systémy SYSTÉM UNIX a Linux</p>	<p>Nastavte nebo změňte cestu k vestavěné běhové vyhledávací cestě (RPath) aplikace.</p> <p>Tato volba vyžaduje opětovnou kompilaci a propojení aplikace. Další informace o kompilaci a propojování aplikací naleznete v tématu Sestavení procedurální aplikace.</p>	<ul style="list-style-type: none"> • Rozsah změny je jasný. 	<ul style="list-style-type: none"> • Musíte být schopni znovu zkompileovat a propojit aplikaci. • Změní-li se umístění IBM MQ , musíte změnit cestu k RPath.
<p>Systémy SYSTÉM UNIX a Linux</p>	<p>Nastavte proměnnou prostředí <code>LD_LIBRARY_PATH</code> (<code>LIBPATH</code> na AIX) pomocí příkazu <code>setmqenv</code> nebo <code>crtmqenvs</code> volbou <code>-k</code> nebo <code>-l</code> .</p>	<ul style="list-style-type: none"> • Nejsou vyžadovány žádné změny v existujících požadovaných aplikacích. • Přepíše vložené cesty RPath v aplikaci. • Snadné změny proměnné, pokud se změní umístění IBM MQ . 	<ul style="list-style-type: none"> • Aplikace <code>setuid</code> a <code>setgid</code> nebo aplikace vytvořené jinými způsoby mohou <code>LD_LIBRARY_PATH</code> ignorovat z bezpečnostních důvodů. • Specifické prostředí musí být nastaveno v každém prostředí, kde je spuštěna aplikace. • Možný dopad na jiné aplikace, které spoléhají na <code>LD_LIBRARY_PATH</code>. • Volby HP-UX: použité při kompilování aplikace mohou zakázat použití proměnné prostředí <code>LD_LIBRARY_PATH</code>. Další informace naleznete v tématu Pokyny týkající se propojení běhového prostředí pro produkt HP-UX. • Linux: Kompilátor používaný k sestavení aplikace může zakázat použití proměnné prostředí <code>LD_LIBRARY_PATH</code>. Další informace naleznete v tématu Pokyny týkající se propojení běhového prostředí pro produkt Linux .

Tabulka 27. Výhody a nevýhody voleb pro načítání knihoven (pokračování)

Platforma	Volba	Výhody	Nevýhody
Systémy Windows	Nastavte proměnnou PATH pomocí příkazu <code>setmqenv</code> nebo <code>crtmqenv</code> .	<ul style="list-style-type: none"> Pro existující aplikace nejsou vyžadovány žádné změny. Snadné změny proměnné, pokud se změní umístění IBM MQ. 	<ul style="list-style-type: none"> Specifické prostředí musí být nastaveno v každém prostředí, kde je spuštěna aplikace. Možný dopad na jiné aplikace.
Systémy SYSTÉM UNIX, Linux a Okna	Nastavte primární instalaci na server Verze 7.1 nebo novější, instalaci. Viz "Změna primární instalace" na stránce 360. Další informace o primární instalaci naleznete v tématu Výběr primární instalace .	<ul style="list-style-type: none"> Pro existující aplikace nejsou vyžadovány žádné změny. Snadná změna primární instalace, pokud se změní umístění IBM MQ. Poskytuje podobné chování jako předchozí verze produktu IBM MQ. 	<ul style="list-style-type: none"> Je-li nainstalován produkt IBM WebSphere MQ 7.0.1, nelze primární instalaci nastavit na verzi Verze 7.1 nebo novější. SYSTÉM UNIX a Linux: Nefunguje, pokud <code>/usr/lib</code> není ve výchozí vyhledávací cestě.

Aspekty implementace knihovny pro produkt HP-UX

Ukázkové příkazy kompilace v dokumentaci produktu pro předchozí verze produktu IBM MQ obsahovaly volbu odkazu `-W1, +noenvvar` pro 64bitové aplikace. Tato volba zakáže použití proměnné prostředí `LD_LIBRARY_PATH` k načtení sdílených knihoven. Pokud chcete, aby aplikace zaváděla knihovny produktu IBM MQ z jiného umístění, než je umístění uvedené v cestě k načtení, musíte aktualizovat své aplikace. Aplikace můžete aktualizovat opětovným kompilováním a propojením bez volby propojení `-W1, +noenvvar`, nebo pomocí příkazu `chattr`.

Chcete-li zjistit, jak vaše aplikace aktuálně načítají knihovny, prohlédněte si téma ["Mechanismy zavádění knihoven operačního systému"](#) na stránce 356.

Aspekty implementace knihovny pro produkt Linux

Aplikace kompilované pomocí některých verzí gcc, například, verze 3.2.x, mohou mít vestavěnou cestu `RPath`, kterou nelze přepsat pomocí proměnné prostředí `LD_LIBRARY_PATH`. Pomocí příkazu `readelf -d applicationName` můžete určit, zda je aplikace ovlivněna. Cestu `RPath` nelze přepsat, je-li přítomen symbol `RPATH` a že není přítomen symbol `RUNPATH`.

Aspekty implementace knihovny pro produkt Solaris

Ukázkové příkazy kompilace v dokumentaci produktu pro předchozí verze produktu IBM MQ obsahovaly volby propojení `-lmqmc` a `-lmqzse`. Odpovídající verze těchto knihoven jsou nyní načteny automaticky produktem IBM MQ. Je-li produkt IBM MQ nainstalován v jiném než výchozím umístění, nebo pokud v systému existuje více instalací, je třeba aktualizovat aplikace. Aplikace můžete aktualizovat opětovným kompilováním a propojením bez voleb odkazu `-lmqmc -lmqzse`.

Mechanismy zavádění knihoven operačního systému

Na systémech Windows se prohledají několik adresářů, kde najdete knihovny:

- Adresář, ze kterého je aplikace načtena.
- Aktuální adresář.
- Adresáře v proměnné prostředí `PATH`, jak globální proměnná `PATH`, tak i proměnná `PATH` aktuálního uživatele.

V systémech SYSTÉM UNIX a Linux existuje řada metod, které mohly být použity k vyhledání knihoven k načtení:

- Pomocí proměnné prostředí `LD_LIBRARY_PATH` (také `LIBPATH` v systému AIXa nastavení `SHLIB_PATH` v systému HP-UX). Je-li tato proměnná nastavena, definuje sadu adresářů, které se prohledají pro požadované knihovny IBM MQ . Pokud jsou v těchto adresářích nalezeny nějaké knihovny, používají se v předvolbách všech knihoven, které by mohly být nalezeny pomocí jiných metod.
- Použití vestavěné vyhledávací cesty (RPath). Aplikace může obsahovat sadu adresářů, které se mají prohledávat kvůli knihovnám IBM MQ . Pokud není proměnná `LD_LIBRARY_PATH` nastavena, nebo pokud požadované knihovny nebyly nalezeny pomocí proměnné, prohledá se cesta RPath pro knihovny. Pokud vaše existující aplikace používají RPath, ale aplikaci nemůžete překompilovat a propojit, musíte buď nainstalovat produkt IBM WebSphere MQ 7.1 do výchozího umístění, nebo použít jinou metodu k vyhledání knihoven.
- Použije se výchozí cesta ke knihovně. Pokud se knihovny produktu IBM MQ nenaleznou po prohledání proměnné `LD_LIBRARY_PATH` a umístění RPath, prohledá se výchozí cesta ke knihovně. Tato cesta obvykle obsahuje `/usr/lib` nebo `/usr/lib64`. Nejsou-li knihovny nalezeny po prohledání předvolené cesty ke knihovně, spuštění aplikace se nezdaří kvůli chybějícím závislostem.

Můžete použít mechanismus operačního systému, abyste zjistili, zda vaše aplikace mají vestavěnou vyhledávací cestu. Příklad:

- AIX: **dump**
- HP-UX: **chatr**
- Linux: **readelf**
- Solaris: **elfdump**

Související pojmy

[“Přidružení správce front k instalaci” na stránce 362](#)

Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému SYSTÉM UNIX, Linuxa Oknamůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

[“Omezení pro aplikace používající více instalací” na stránce 357](#)

Existují omezení při použití knihoven serveru produktu CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními podmínkami.

[“Připojování aplikací v prostředí s více instalačními prostředí” na stránce 352](#)

On SYSTÉM UNIX, Linuxa Okna systems, if IBM WebSphere MQ 7.1, or later, libraries are loaded, IBM MQ automatically uses the appropriate libraries without you needing to take any further action. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Související úlohy

[“Změna primární instalace” na stránce 360](#)

K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz **setmqinst** .

Související informace

[Výběr primární instalace](#)

Omezení pro aplikace používající více instalací

Existují omezení při použití knihoven serveru produktu CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními podmínkami.

Knihovny serveru CICS

Používáte-li knihovny serveru CICS , produkt IBM MQ pro vás automaticky nevybere správnou úroveň knihovny. Musíte zkompileovat a propojit aplikace s příslušnou úrovní knihovny pro správce front, ke kterému se aplikace připojuje. Další informace naleznete v tématu [Sestavování knihoven pro použití s produktem TXSeries for Multiplatforms verze 5](#).

Obslužné rutiny zpráv

Popisovače zpráv, které používají speciální hodnotu MQHC_UNASSOCIATED_HCONN, jsou omezeny na použití při první instalaci načtené do procesu. Pokud obslužnou rutinu zpráv nemůže použít konkrétní instalace, je vrácen kód příčiny MQRC_HMSG_NOT_AVAILABLE.

Toto omezení ovlivňuje vlastnosti zprávy. Obslužné rutiny zpráv nelze použít k získání vlastností zprávy od správce front v rámci jedné instalace a jejich umístění do správce front v jiné instalaci. Další informace o obslužných rutinách zpráv naleznete v tématu [MQCRTMH-Create message handle](#).

Uživatelské procedury

V prostředí s více instalacemi musí být existující uživatelské procedury aktualizovány pro použití s instalacemi produktu IBM WebSphere MQ 7.1 nebo novější. Uživatelské procedury pro převod dat vygenerované pomocí příkazu **crtmqcvx** musí být znovu generovány s použitím aktualizovaného příkazu.

Všechny uživatelské procedury musí být zapsány pomocí struktury MQIEP, nelze použít vestavěný RPATH k vyhledání knihoven produktu IBM MQ a nemohou se odkazovat na knihovny IBM MQ. Další informace najdete v tématu [Psaní výstupních vstupů a instalovatelných služeb na UNIX, Linux a Windows](#).

Rychlý způsob

Na serveru s více instalacemi musí aplikace používající připojení rychlým způsobem k IBM WebSphere MQ verze 7.1 nebo novějšímu splňovat tato pravidla:

1. Správce front musí být přidružen ke stejné instalaci jako ten, ze kterého aplikace načte běhové knihovny IBM MQ. Aplikace nesmí používat připojení rychlým způsobem ke správci front přidruženému k jiné instalaci. Pokus vytvořit připojení vede k chybě a kódu příčiny MQRC_INSTALLATION_MISMATCH.
2. Připojení jinak než rychlým způsobem ke správci front přidruženému ke stejné instalaci, ze které aplikace načte běhové knihovny IBM MQ, brání aplikaci připojit se rychlým způsobem, pokud neplatí některá z následujících podmínek.
 - Aplikace učiní první připojení ke správci front přidruženému ke stejné instalaci rychlým způsobem připojení.
 - Je nastavena proměnná prostředí AMQ_SINGLE_INSTALLATION.
3. Připojení jinak než rychlým způsobem ke správci front přidruženému k instalaci verze 7.1 nebo novější nemá žádný vliv na to, zda se aplikace může připojit rychlým způsobem.
4. Nemůžete kombinovat připojení ke správci front přidruženému k instalaci verze 7.0.1 s připojením rychlým způsobem ke správci front přidruženému k instalaci verze 7.1 nebo novější.

Máte-li nastaven parametr AMQ_SINGLE_INSTALLATION, můžete učinit jakékoliv připojení ke správci front připojením rychlým způsobem. Jinak platí téměř stejná omezení:

- Instalace musí být stejná jako ta, ze které byly načteny běhové knihovny produktu IBM MQ.
- Všechna připojení k jednomu procesu musí být ke stejné instalaci. Pokud se pokusíte připojit ke správci front přidruženému k jiné instalaci, připojení se nezdaří s kódem příčiny MQRC_INSTALLATION_MISMATCH. Uvědomte si, že je-li nastaven parametr AMQ_SINGLE_INSTALLATION, platí toto omezení pro všechna připojení, a ne pouze pro připojení rychlým způsobem.
- Připojte pouze jednoho správce front s připojeními rychlým způsobem.

Související informace

[MQCONN- Připojit správce front \(rozšířený\)](#)

[Struktura MQIEP](#)

[2583 \(0A17\) \(RC2583\): Rozhraní MQRC_INSTALLATION_MISMATCH](#)

[2587 \(0A1B\) \(RC2587\): MQRC_HMSG_NOT_AVAILABLE](#)

[2590 \(0A1E\) \(RC2590\): MQRC_FASTPATH_NOT_AVAILABLE](#)

Připojení aplikací produktu .NET v prostředí s více instalačními prostředí

Při výchozím nastavení aplikace používají montážní celky .NET z primární instalace. Pokud neexistuje žádná primární instalace, nebo nechcete použít žádné primární montážní celky, musíte aktualizovat konfigurační soubor aplikace nebo proměnnou prostředí *DEVPATH*.

Je-li v systému primární instalace, jsou soubory .NET a soubory zásad této instalace zaregistrovány do globální mezipaměti sestavení (GAC). Sestavy .NET pro všechny ostatní instalace lze najít v instalační cestě každé instalace, ale sestavy nejsou registrovány v GAC. Proto se aplikace standardně spouštějí s použitím montážních celků .NET z primární instalace. Konfigurační soubor aplikace je třeba aktualizovat, je-li splněna některá z následujících podmínek:

- Nemáte primární instalaci.
- Nechcete, aby aplikace používala montážní celky primárních instalací.
- Primární instalace je nižší verze produktu IBM MQ než verze, se kterou byla aplikace zkompileována.

Informace o tom, jak aktualizovat konfigurační soubor aplikací, viz [“Připojení aplikací produktu .NET s použitím konfiguračního souboru aplikace”](#) na stránce 359.

Proměnnou prostředí *DEVPATH* je třeba aktualizovat, je-li splněna následující podmínka:

- Chcete, aby aplikace používala sestavy z jiné než primární instalace, ale primární instalace je na stejné verzi jako nepřimární instalace.

Další informace o tom, jak aktualizovat proměnnou *DEVPATH* viz [“Připojení aplikací .NET pomocí DEVPATH”](#) na stránce 360.

Připojení aplikací produktu .NET s použitím konfiguračního souboru aplikace

V konfiguračním souboru aplikace je třeba nastavit různé značky pro přesměrování aplikací tak, aby používaly sestavy, které nejsou z primární instalace.

V následující tabulce jsou uvedeny specifické změny, které je třeba provést v konfiguračním souboru aplikací, aby se aplikace .NET připojily pomocí konkrétních sestav:

	Aplikace kompilované se starší verzí produktu IBM MQ	Aplikace kompilované s novější verzí produktu IBM MQ
Chcete-li spustit aplikaci s vyšší verzí produktu IBM MQ, primární instalací. (novější verze sestav v GAC):	Nejsou nutné žádné změny	Nejsou nutné žádné změny
Chcete-li spustit aplikaci se starší verzí produktu IBM MQ, primární instalací. (předchozí sestavy verzí v GAC):	Nejsou nutné žádné změny	V konfiguračním souboru aplikace: <ul style="list-style-type: none">• Použijte značku <code><bindingRedirect></code> k označení použití dřívější verze sestav, které jsou v GAC.
Chcete-li spustit aplikaci s novější verzí produktu IBM MQ, která není primární, použijte jinou než primární instalaci. (novější verze sestav v instalační složce):	V konfiguračním souboru aplikace: <ul style="list-style-type: none">• Použijte značku <code><codebase></code> k umístění na umístění sestav pozdějších verzí• Použijte značku <code><bindingRedirect></code> k označení použití sestav s novější verzí.	V konfiguračním souboru aplikace: <ul style="list-style-type: none">• Použijte značku <code><codebase></code> k umístění na umístění sestav pozdějších verzí

Tabulka 28. Konfigurace aplikací pro použití konkrétních sestav (pokračování)

	Aplikace kompilované se starší verzí produktu IBM MQ	Aplikace kompilované s novější verzí produktu IBM MQ
Chcete-li spustit aplikaci se starší verzí produktu IBM MQ, než je primární instalace. (předchozí sestavy verzí v instalační složce):	<p>V konfiguračním souboru aplikace:</p> <ul style="list-style-type: none"> • Použijte značku <code><codebase></code> k umístění do umístění sestav starších verzí • Zahrnout značku <code><publisherpolicy Apply=no></code> 	<p>V konfiguračním souboru aplikace:</p> <ul style="list-style-type: none"> • Použijte značku <code><codebase></code> k umístění do umístění sestav starších verzí • Značku <code><bindingRedirect></code> použijte k označení použití sestav předchozí verze • Zahrnout značku <code><publisherpolicy Apply=no></code>

Ukázkový konfigurační soubor aplikace `NonPrimaryRedirect.config` se dodává ve složce `MQ_INSTALLATION_PATH\tools\dotnet\samples\base`. Tento soubor může být upraven pomocí instalační cesty produktu IBM MQ jakékoli jiné než primární instalace. Soubor může být také přímo zahrnut do jiných konfiguračních souborů pomocí značky `<linkedConfiguration>`. Ukázky jsou k dispozici pro produkty `nmqsget.exe.config` a `nmqsput.exe.config`. Oba ukázky používají značku `<linkedConfiguration>` a obsahují soubor `NonPrimaryRedirect.config`.

Připojení aplikací .NET pomocí DEVPATH

Sestavy můžete najít pomocí proměnné prostředí `DEVPATH`. Sestavy uvedené v proměnné `DEVPATH` se používají jako předvolba pro všechny sestavy v GAC. Další informace o tom, kdy použít tuto proměnnou, najdete v příslušné dokumentaci produktu Microsoft v souboru `DEVPATH`.

Chcete-li vyhledat sestavy pomocí proměnné prostředí `DEVPATH`, musíte nastavit proměnnou `DEVPATH` na složku, která obsahuje sestavy, které chcete použít. Poté je třeba aktualizovat konfigurační soubor aplikace a přidat následující informace o konfiguraci běhového prostředí:

```
<configuration>
<runtime>
<developmentMode developerInstallation="true" />
</runtime>
</configuration>
```

Související pojmy

[“Připojování aplikací v prostředí s více instalačními prostředí” na stránce 352](#)

On SYSTEM UNIX, Linuxa Okna systems, if IBM WebSphere MQ 7.1, or later, libraries are loaded, IBM MQ automatically uses the appropriate libraries without you needing to take any further action. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Související informace

[Výběr primární instalace](#)

[použití.NET](#)

[Více instalací](#)

Změna primární instalace

K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz `setmqinst`.

Informace o této úloze

Tato úloha se týká produktu SYSTEM UNIX, Linuxa Okna.

Primární instalace je instalace, na kterou se odkazují požadované umístění v celém systému. Další informace o primární instalaci a pokyny k výběru primární instalace naleznete v tématu [Výběr primární instalace](#).

Je-li instalace produktu IBM WebSphere MQ 7.1 nebo novější koexistence s instalací produktu IBM WebSphere MQ 7.0.1, instalace produktu IBM WebSphere MQ 7.0.1 musí být primární. Je označen jako primární, je-li nainstalována verze produktu IBM WebSphere MQ 7.1 nebo vyšší, a instalaci produktu IBM WebSphere MQ 7.1 nebo novější nelze provést jako primární.

Během procesu instalace v systému Windows můžete určit, že se má instalace primární instalací. Na systémech SYSTÉM UNIX a Linux musíte po instalaci zadat příkaz **setmqinst**, který nastaví instalaci jako primární instalaci.

[“Nastavit primární instalaci” na stránce 361.](#)

[“Zrušit nastavení primární instalace” na stránce 361.](#)

Nastavit primární instalaci

Postup

Chcete-li nastavit instalaci jako primární instalaci, postupujte takto:

1. Zkontrolujte, zda je instalace již primární instalací, zadáním následujícího příkazu:

```
MQ_INSTALLATION_PATH/bin/dspmqinst
```

kde *MQ_INSTALLATION_PATH* je instalační cesta k instalaci produktu IBM WebSphere MQ 7.1 nebo pozdější.

2. Je-li existující instalace produktu IBM WebSphere MQ 7.1 nebo novější nastavena jako primární instalace, zrušte její nastavení podle pokynů v části [“Zrušit nastavení primární instalace” na stránce 361](#). Je-li v systému nainstalován produkt IBM WebSphere MQ 7.0.1, nelze primární instalaci změnit.
3. Jako uživatel root v systémech SYSTÉM UNIX a Linux nebo člen skupiny Administrators v systémech Windows zadejte jeden z následujících příkazů:

- Chcete-li nastavit primární instalaci pomocí cesty k instalaci, kterou chcete použít jako primární instalaci, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -i -p MQ_INSTALLATION_PATH
```

- Chcete-li nastavit primární instalaci pomocí názvu instalace, kterou chcete provést jako primární, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -i -n installationName
```

4. V systémech Windows restartujte systém.

Zrušit nastavení primární instalace

Postup

Chcete-li zrušit nastavení instalace jako primární instalace, postupujte takto:

1. Zkontrolujte, která instalace je primární instalací, zadáním následujícího příkazu:

```
MQ_INSTALLATION_PATH/bin/dspmqinst
```

kde *MQ_INSTALLATION_PATH* je instalační cesta k instalaci produktu IBM WebSphere MQ 7.1 nebo pozdější.

Je-li IBM WebSphere MQ 7.0.1 primární instalací, nemůžete zrušit nastavení primární instalace.

2. Jako uživatel root v systémech SYSTÉM UNIX a Linux nebo člen skupiny Administrators v systémech Windows zadejte jeden z následujících příkazů:

- Chcete-li zrušit nastavení primární instalace pomocí cesty k instalaci, již nadále nechcete být primární instalací, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -x -p MQ_INSTALLATION_PATH
```

- Chcete-li zrušit nastavení primární instalace s použitím názvu instalace, již nadále nechcete být primární instalací, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -x -n installationName
```

Související informace

[Funkce, které lze použít pouze s primární instalací v systému Windows](#)

[Odkazy na externí knihovny a řídicí příkaz pro primární instalaci v systému SYSTÉM UNIX a Linux](#)

[Odinstalování, upgrade a údržba primární instalace](#)

[Výběr názvu instalace](#)

[setmqinst](#)

Přidružení správce front k instalaci

Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm**. V systému SYSTÉM UNIX, Linuxu můžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm**.

Příkaz **setmqm** lze použít následujícími způsoby:

- Přesun jednotlivých správců front mezi rovnocennými verzemi produktu IBM MQ. Například přesun správce front z testovacího do produkčního systému.
- Migrace jednotlivých správců front ze starší verze produktu IBM MQ na novější verzi produktu IBM MQ. Migrace správců front mezi verzemi má různé důsledky, o kterých si musíte být vědomi. Další informace o migraci naleznete v tématu [Migrace a upgrade produktu IBM MQ](#).

Chcete-li přidružit správce front k instalaci, postupujte takto:

1. Zastavte správce front pomocí příkazu **endmqm** z instalace, která je aktuálně asociována se správcem front.
2. Přidružte správce front k jiné instalaci pomocí příkazu **setmqm** z této instalace.

Chcete-li například nastavit správce front QMB tak, aby byl přidružen k instalaci s názvem `Installation2`, zadejte do adresáře `Installation2`: tento příkaz:

```
MQ_INSTALLATION_PATH/bin/setmqm -m QMB -n Installation2
```

kde `MQ_INSTALLATION_PATH` je cesta, kde je nainstalována `Installation2`.

3. Spusťte správce front pomocí příkazu **strmqm** z instalace, která je nyní přidružena ke správci front.

Tento příkaz provede nezbytnou migraci správce front a jeho výsledky budou připraveny k použití správcem front.

Instalace, ke které je správce front přidružen, omezuje správce front tak, aby mohl být spravován pouze příkazy z této instalace. Existují tři klíčové výjimky:

- Produkt **setmqm** mění instalaci přidruženou ke správci front. Tento příkaz musí být zadán z instalace, kterou chcete přidružit ke správci front, nikoli k instalaci, k níž je aktuálně přidružen správce front. Název instalace zadaný příkazem **setmqm** musí odpovídat instalaci, ze které se příkaz vydal.
- **strmqm** je obvykle nutné zadat z instalace, která je přidružena ke správci front. Když se však správce front verze V7.0.1 nebo starší spustí poprvé v systému V7.1 nebo novější, lze použít příkaz **strmqm**.

V takovém případě produkt **strmqm** spustí správce front a přidruží jej k instalaci, ze které je příkaz zadán.

- Produkt **dspmq** zobrazuje informace o všech správcích front v systému, nikoli pouze o těch správcích front přidružených ke stejné instalaci jako příkaz **dspmq -o installation** zobrazí informace o tom, které správci front jsou přidruženi k instalacím.

Přidružení správce front v prostředí s vysokou dostupností

Pro prostředí HA příkaz **addmqinf** automaticky asociuje správce front s instalací, ze které je příkaz **addmqinf** zadán. Pokud je příkaz **strmqm** zadán ze stejné instalace jako příkaz **addmqinf**, není třeba žádné další nastavení. Chcete-li spustit správce front pomocí jiné instalace, je třeba nejprve změnit přidruženou instalaci pomocí příkazu **setmqm**.

Správci front přidružení k odstraněným instalacím

Je-li instalace, ke které je přidružen správce front, odstraněna, nebo pokud jsou informace o stavu správce front nedostupné, příkaz **setmqm** nepřidruží správce front k jiné instalaci. V této situaci proveďte následující akce:

1. Použijte příkaz **dspmqinst**, abyste viděli ostatní instalace na vašem systému.
2. Ručně upravte pole `InstallationName` oddílu `QueueManager` v souboru `mq.ini` tak, aby určoval jinou instalaci.
3. K odstranění správce front použijte příkaz **dlmqm** z této instalace.

Související pojmy

[“Vyhledání instalací produktu IBM MQ v systému” na stránce 363](#)

Máte-li v systému více instalací produktu IBM MQ, můžete zkontrolovat, které verze jsou nainstalované a kde jsou.

[“Konfigurační soubor IBM MQ, mq.ini.” na stránce 83](#)

Konfigurační soubor IBM MQ `mq.ini` obsahuje informace vztahující se ke všem správcům front v daném uzlu. Vytvoří se automaticky během instalace.

Související informace

[Výběr primární instalace](#)

[setmqm](#)

[strmqm](#)

[dspmq](#)

[dspmqinst](#)

Vyhledání instalací produktu IBM MQ v systému

Máte-li v systému více instalací produktu IBM MQ, můžete zkontrolovat, které verze jsou nainstalované a kde jsou.

Při hledání instalací produktu IBM MQ ve vašem systému můžete použít následující metody:

- Použijte příkaz **dspmqver**. Tento příkaz neposkytuje podrobné informace o všech instalacích v systému, pokud je tento příkaz vydán z instalace produktu Verze 7.0.1.
- Použijte instalační nástroje platformy pro dotaz, kde byl nainstalován produkt IBM MQ. Potom použijte příkaz **dspmqver** z instalace produktu Verze 7.1 nebo novější. Následující příkazy jsou příklady příkazů, které můžete použít k dotazování tam, kde byl nainstalován produkt IBM MQ:
 - V systémech AIX můžete použít příkaz **lslpp**:

```
lslpp -R ALL -l mqm.base.runtime
```

- V systémech HP-UX můžete použít příkaz **swlist** :

```
swlist -a location -a revision -l product MQSERIES
```

- V systémech Linux můžete použít příkaz **rpm** :

```
rpm -qa --qf "%{NAME}-%{VERSION}-%{RELEASE}\t%{INSTPREFIXES}\n" | grep MQSeriesRuntime
```

- V systémech Solaris můžete použít příkazy **pkginfo** a **pkgparam** :

1. Seznam instalovaných balíčků lze vypsat zadáním následujícího příkazu:

```
pkginfo | grep -w mqm
```

2. Pro každý vypsaný balík zadejte následující příkaz:

```
pkgparam pkgname BASEDIR
```

- V systémech Windows můžete použít příkaz **wmic** . Tento příkaz může instalovat klienta wmic:

```
wmic product where "(Name like 'MQ%') AND (not Name like '%bitSupport')" get Name, Version, InstallLocation
```

- Na systémech SYSTÉM UNIX a Linux zadejte následující příkaz, abyste zjistili, kde je nainstalován produkt IBM MQ :

```
cat /etc/opt/mqm/mqinst.ini
```

Potom použijte příkaz **dspmqr** z instalace produktu Verze 7.1 nebo novější.

- Chcete-li zobrazit podrobnosti o instalacích na systému na 32bitovém systému Windows, zadejte následující příkaz:

```
reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere MQ\Installation" /s
```

- V 64bitovém systému Windowszadejte následující příkaz:

```
reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IBM\WebSphere MQ\Installation" /s
```

Poznámka: příkaz **reg.exe** zobrazí pouze informace o instalaci produktu Verze 7.1 nebo pozdější.

Související informace

[dspmqr](#)

[dspmqinst](#)


[Více instalací](#)


Dostupnost, obnova a restartování

Zpřístupněte si své aplikace tím, že zachovají dostupnost fronty, pokud správce front selže, a po selhání serveru nebo úložiště obnovte zprávy.

Zlepšete dostupnost aplikací klienta pomocí opětovného připojení klienta k přepnutí klienta automaticky mezi skupinou správců front nebo novou aktivní instancí správce front s více instancemi po selhání správce front. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

 Zvyšte dostupnost aplikací serveru v produktu z/OS pomocí skupin sdílení front.

V systémech Windows,  IBM i, UNIXa Linux implementují serverové aplikace do správce front s více instancemi, který je konfigurován tak, aby se spouštěl jako jeden správce front na více serverech; pokud server, na kterém běží aktivní instance, selže, je provedení automaticky přepnuto na záložní instanci stejného správce front na jiném serveru. Pokud nakonfigurujete serverové aplikace tak, aby se spouštěly jako služby správce front, restartují se, když se rezervní instance stane aktivně spuštěnou instancí správce front.

Produkt IBM MQ můžete nakonfigurovat jako součást řešení klastrování specifického pro platformu, například Microsoft Cluster Server,  HA clusters on IBM i, nebo PowerHA for AIX (dříve HACMP na AIX). a další klastrová řešení SYSTÉM UNIX a Linux.

Další možnosti, jak zvýšit dostupnost serverové aplikace, je implementovat serverové aplikace na více počítačů v klastru správců front.

Systém zasílání zpráv zajišťuje, že zprávy zadané do systému budou doručeny do místa určení. Produkt IBM MQ může trasovat přenosovou cestu ke zprávě při přesunu z jednoho správce front do jiného pomocí příkazu **dspmqrte**. Dojde-li k selhání systému, mohou být zprávy obnoveny různými způsoby v závislosti na typu selhání a způsobu, jakým je systém nakonfigurován.

Produkt IBM MQ zajišťuje, že zprávy nebudou ztraceny zachováním protokolů o zotavení aktivit správců front, kteří obsluhují příjemce, přenos a doručování zpráv. Využívá tyto protokoly pro tři typy obnovy:

1. *Restartovat obnovu*, když zastavujete IBM MQ v plánovaném způsobu.
2. *Zotavení po selhání*, pokud se selhání zastaví IBM MQ.
3. *Obnova médií*, chcete-li obnovit poškozené objekty.

Ve všech případech obnova obnoví správce front do stavu, v němž se nacházela při zastavení správce front s tím rozdílem, že všechny transakce v době letu byly odvolány a odebrány z front všechny aktualizace, které byly v době zastavení správce front k dispozici v době zastavení. Obnova obnoví všechny trvalé zprávy, přechodné zprávy mohou být během procesu ztraceny.

Automatické opětovné připojení klienta

Můžete provést automatické opětovné připojení klientských aplikací, aniž byste zapisoval nějaký dodatečný kód, a to konfigurací počtu komponent.

Automatické opětovné připojení klienta je *vloženo*. Toto připojení se automaticky obnoví v každém okamžiku aplikačního programu klienta a obnoví se všechny popisovače k otevřeným objektům.

Naopak ruční opětovné připojení vyžaduje, aby aplikace klienta znovu vytvořila připojení pomocí MQCONN nebo MQCONNX a znovu otevřela objekty. Automatické opětovné připojení klienta je vhodné pro řadu aplikací klienta, nikoliv však pro všechny.

Tabulka 29 na stránce 366 uvádí nejstarší vydání podpory klienta IBM MQ, které musí být nainstalováno na pracovní stanici klienta. Pracovní stanice klienta je třeba převést na jednu z těchto úrovní pro aplikaci, která má používat automatické opětovné připojení klienta. Tabulka 30 na stránce 366 vypíše další požadavky, které umožní automatické opětovné připojení klienta.

Při přístupu programu k volbám opětovného připojení může klientská aplikace nastavit možnosti opětovného připojení. S výjimkou klientů JMS a XMS, má-li klientská aplikace přístup k volbám opětovného připojení, může také vytvořit obslužnou rutinu událostí pro obsluhu událostí opětovného připojení.

Existující klientská aplikace může mít prospěch z podpory opětovného připojení, bez rekompilace a linkování:

- V případě klienta jiného typu než JMS nastavte proměnnou prostředí `mqcClient.ini DefRecon` na nastavení možností opětovného připojení. Použijte tabulku CCDT pro připojení ke správci front. Pokud se má klient připojit ke správci front s více instancemi, zadejte síťové adresy aktivních a rezervních instancí správce front v tabulce CCDT.
- Pro klienta produktu JMS nastavte volby opětovného připojení v konfiguraci továrny připojení. Při spuštění v kontejneru EJB serveru Java EE se objekty MDB mohou znovu připojit k produktu IBM MQ

pomocí mechanismu opětovného připojení poskytovaného aktivačními specifikacemi adaptéru prostředků produktu IBM MQ (nebo portů modulu listener, jsou-li spuštěny v produktu WebSphere Application Server). Pokud však aplikace není MDB (nebo je spuštěna ve webovém kontejneru), aplikace musí implementovat svou vlastní logiku opětovného připojení, protože automatické opětovné připojení klienta není v tomto scénáři podporováno. Adaptér prostředků produktu IBM MQ poskytuje tuto schopnost opětovného připojení pro doručování zpráv do objektů typu message-driven bean, ale jiné prvky produktu Java EE, jako jsou servlety, musí implementovat vlastní opětovné připojení.

Poznámka: Automatické opětovné připojení klienta není podporováno produktem IBM MQ classes for Java.

<i>Tabulka 29. Podporovaní klienti</i>			
Rozhraní klienta	Klient	Přístup k programu pro volby opětovného připojení	Podpora opětovného připojení
Rozhraní API systému	C, C + +, COBOL, Nespravovaný Visual Basic, XMS (Nespravované XMS na Windows)	7.0.1	7.0.1
	Kontejner JMS (Kontejner klienta JSE a Java EE a spravované kontejnery)	7.0.1.3	7.0.1.3
	IBM MQ classes for Java	Nepodporováno	Nepodporováno
	Spravované klienty XMS a spravované klienti .NET : C#, Visual Basic,	7.1	7.1
Jiná rozhraní API	Windows Communication Foundation (Nespravovaný ¹)	Nepodporováno	7.0.1
	Windows Communication Foundation (Spravováno ¹)	Nepodporováno	Nepodporováno
	Osa 1	Nepodporováno	Nepodporováno
	Osa 2	Nepodporováno	7.0.1.3
	HTTP (web 2.0)	Nepodporováno	7.0.1.3

1. Nastavení spravovaného nebo nespravovaného režimu v konfiguraci vazby WCF.

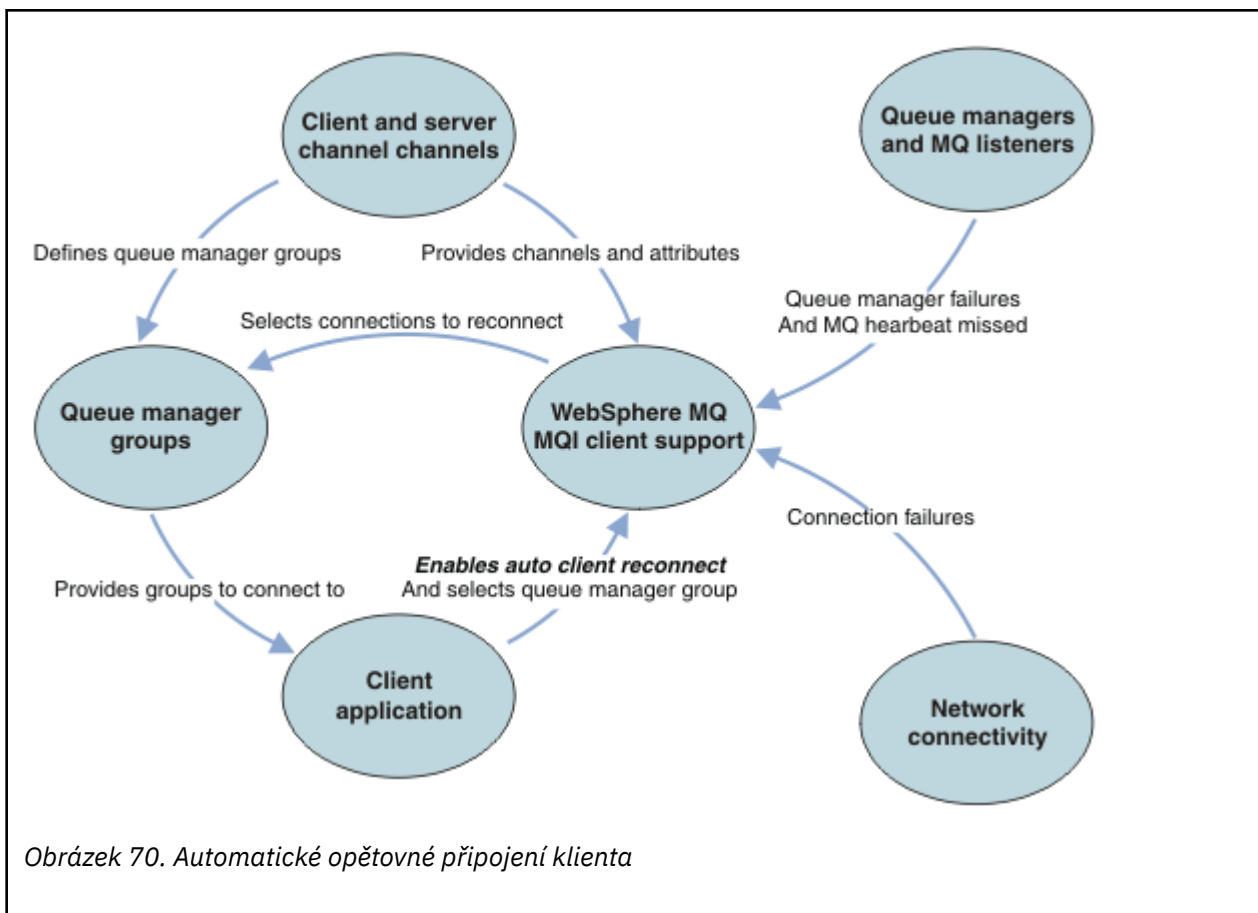
Automatické opětovné připojení má následující požadavky na konfiguraci:

<i>Tabulka 30. Požadavky na konfiguraci automatického opětovného připojení</i>		
Komponenta	Požadavek	Vliv nesplnění požadavku
instalace produktu IBM MQ MQI client	Viz téma Tabulka 29 na stránce 366	MQRC_OPTIONS_ERROR
Instalace serveru IBM MQ	Úroveň 7.0.1	MQRC_OPTIONS_ERROR
Kanál	SHARECNV > 0	MQRC_ENVIRONMENT_ERROR
prostředí aplikace	Musí být vláknový	MQRC_ENVIRONMENT_ERROR

Tabulka 30. Požadavky na konfiguraci automatického opětovného připojení (pokračování)

Komponenta	Požadavek	Vliv nesplnění požadavku
MQI	<p>Jedna z možností:</p> <ul style="list-style-type: none"> MQCONN s volbami MQCNE Volby nastaveným na hodnotu MQCNO_RECONNECT nebo MQCNO_RECONNECT_Q_MGR. Defrecon=YES QMGR je v mqclient.ini V produktu JMS nastavte vlastnost CLIENTRECONOPTIONS továrny připojení. 	MQCC_FAILED je-li připojení přerušeno nebo selže nebo selže správce front.

Produkt [Obrázek 70 na stránce 367](#) zobrazuje hlavní interakce mezi komponentami, které jsou zapojeny do opětovného připojení klienta.



Aplikace klienta

Klientská aplikace je IBM MQ MQI client.

- Ve výchozím nastavení nejsou klienti automaticky znovu připojeni. Povolte automatické opětovné připojení klienta nastavením volby MQCONN MQCNO Option MQCNO_RECONNECT nebo MQCNO_RECONNECT_Q_MGR.
- Mnoho aplikací je napsáno takovým způsobem, že jsou schopni využít výhod automatického opětovného připojení bez dalšího kódování. Povolte automatické opětovné připojení pro existující programy, bez

provedení jakýchkoli změn kódu, nastavením atributu DefRecon ve stanze kanálů konfiguračního souboru mqclient.ini.

- Použijte jednu z těchto tří voleb:

1. Upravte program tak, aby logika nebyla ovlivněna opětovným připojením. Například může být nutné volat volání MQI v rámci synchronizačního bodu a znovu odeslat zálohované transakce.
2. Přidejte obslužnou rutinu událostí pro zjištění opětovného připojení a obnovte stav aplikace klienta při opětovném navázání připojení.
3. Nepovolit automatické opětovné připojení: namísto toho odpojte klienta a zadejte nové volání MQI produktu MQCONN nebo MQCONNX k nalezení jiné instance správce front, která je spuštěna ve stejné skupině správců front.

Další podrobnosti o těchto třech volbách naleznete v tématu [“Obnova aplikace”](#) na stránce 451.

- Opětovné připojení ke správci front se stejným názvem nezaručuje, že jste se znovu připojili ke stejné instanci správce front.

Použijte volbu MQCNO MQCNO_RECONNECT_Q_MGR, chcete-li se znovu připojit k instanci stejného správce front.

- Klient může registrovat obslužnou rutinu událostí tak, aby mohl být informován o stavu opětovného připojení. MQHCONN poslanou v obslužné rutině událostí nelze použít. K dispozici jsou následující kódy příčiny:

PŘIPOJENÍ MQRC_RECONNECTING

Připojení se nezdařilo a systém se pokouší znovu navázat spojení. Pokud je provedeno více pokusů o opětovné připojení, obdržíte více událostí produktu MQRC_RECONNECTING.

MQRC_RECONNECTED

Provedené opětovné připojení a všechny obslužné rutiny byly úspěšně znovu vytvořeny.

SELHÁNÍ OPERACE MQRC_RECONNECT_FAILED

Nové připojení nebylo úspěšné.

FUNKCE MQRC_RECONNECT_QMID_MISMATCH

Bylo zadáno připojení s možností opětovného připojení MQCNO_RECONNECT_Q_MGR a připojení se pokusilo znovu připojit k jinému správci front.

POŽ. Q_MGR_QM_Q_MGR_QM_Q_MGR_

V klientském programu, který vyžaduje opětovné připojení ke stejnému správci front, byla v klientském programu uvedena volba, například MQMO_MATCH_MSG_TOKEN ve volání MQGET.

- Reconnectable klient je schopen znovu připojit automaticky pouze po připojení. To znamená, že volání MQCONNX samo o sobě se nepokusí znovu, pokud selže. Pokud například obdržíte návratový kód 2543 - MQRC_STANDBY_Q_MGR z MQCONNX, znovu zadejte volání po krátké prodlevě.

MQRC_RECONNECT_INCOMPATIBLE

Tento kód příčiny je vrácen při pokusu aplikace o použití produktu MQPMO_LOGICAL_ORDER (příkazy MQPUT a MQPUT1) nebo MQGMO_LOGICAL_ORDER (s MQGET). Jsou-li nastaveny volby opětovného připojení. Důvod vrácení kódu příčiny spočívá v tom, že aplikace se v takových případech nikdy znovu nevyužívají.

MQRC_CALL_INTERRUPTED

Tento kód příčiny je vrácen při přerušení připojení během provádění volání Commit a opětovného připojení klienta. MQPUT trvalé zprávy mimo synchronizační bod má za následek vrácení kódu příčiny do aplikace.

Správci front s více instancemi

Zjednodušuje restartování aplikací produktu IBM MQ MQI client poté, co správce front s více instancemi aktivoval svou instanci v pohotovostním režimu, a to pomocí automatického opětovného připojení klienta.

Rezervní instance správce front s více instancemi se obvykle nachází na jiné síťové adrese pro aktivní instanci. Zahrnout síťové adresy obou instancí v tabulce definic připojení klienta (CCDT). Zadejte buď

seznam síťových adres pro parametr **CONNAME** , nebo definujte více řádků pro správce front v tabulce CCDT.

Běžně se produkt IBM MQ MQI clients znovu připojí ke kterémukoli správci front ve skupině správců front. Někdy chcete, aby se produkt IBM MQ MQI client znovu připojil pouze ke stejnému správci front. Může mít afinitu ke správci front. Klienta můžete zabránit tak, aby se znovu připojil k jinému správci front. Nastavte volbu MQCNO , MQCNO_RECONNECT_Q_MGR. Pokud se produkt IBM MQ MQI client znovu připojí k jinému správci front, dojde k selhání. Nastavíte-li volbu MQCNO , MQCNO_RECONNECT_Q_MGR, nezahrnujte do stejné skupiny správců front další správce front. Klient vrátí chybu, pokud se správce front, k němuž se znovu připojuje, nejedná o stejného správce front jako ten, k němuž je připojen.

Skupiny správců front

Můžete vybrat, zda se klientská aplikace vždy připojí a znovu připojí ke správci front se stejným názvem, ke stejnému správci front nebo k některé ze sady správců front, které jsou definovány se stejnou hodnotou QMNAME v tabulce připojení klienta.

- The queue manager *Název* attribute, **NÁZEV** QMNAME, in the client channel definition is the name of a queue manager group.
- Pokud v aplikaci klienta nastavíte hodnotu parametru MQCONN nebo MQCONNX QmgrName na název správce front, připojí se klient pouze ke správcům front s tímto názvem. Pokud zadáte předponu názvu správce front s hvězdičkou (*), klient se připojí ke kterémukoli správci front ve skupině správců front se stejnou hodnotou proměnné QMNAME . Úplné vysvětlení naleznete v tématu [Skupiny správců front](#) v tabulce CCDT.

Skupiny sdílení front

Automatické opětovné připojení klienta ke skupinám sdílení front produktu z/OS používá stejné mechanismy pro opětovné připojení jako kterékoli jiné prostředí. Klient se znovu připojí ke stejnému výběru správců front, jak je nakonfigurováno pro původní připojení. Například při použití tabulky definic kanálů klienta by měl administrátor zajistit, aby všechny záznamy v tabulce byly interpretovatelné na stejnou skupinu sdílení front produktu z/OS .

Definice kanálů klienta a serveru

Definice kanálů klienta a serveru definují skupiny správců front, ke kterým se může klientská aplikace znovu připojit. Definice řídí výběr a časování opětovného připojení a další faktory, jako např. zabezpečení; viz související témata. Nejrelevantnější atributy kanálu, které se mají zvážit pro opětovné připojení, jsou vypsány ve dvou skupinách:

Atributy připojení klienta

Afinita připojení (AFFINITY) AFFINITY

Příbuznost připojení.

Váha kanálu klienta (CLNTWGHT) CLNTWGHT

Váha připojení klienta.

Název připojení (CONNAME) CONNAME

Informace o připojení.

Interval prezenčního signálu (HBINT) HBINT

Interval prezenčního signálu. Nastavte interval prezenčního signálu na kanálu připojení serveru.

Interval udržení aktivity (KAINT) KAINIT

Interval udržení aktivity. Nastavte interval udržení aktivity na kanálu připojení serveru.

Všimněte si, že KAINIT se vztahuje pouze na z/OS .

Název správce front (QMNAME) QMNAME

Název správce front.

Atributy připojení serveru

Interval prezenčního signálu (HBINT) HBINT

Interval prezenčního signálu. Nastavte interval prezenčního signálu na kanálu připojení klienta.

Interval udržení aktivity (KAIN) KAIN

Interval udržení aktivity. Nastavte interval udržení aktivity na kanálu připojení klienta.

Všimněte si, že KAIN se vztahuje pouze na z/OS .

KAIN je prezenční signál síťové vrstvy a HBINT je prezenční signál produktu IBM MQ mezi klientem a správcem front. Nastavení těchto synchronizačních signálů po kratší dobu slouží ke dvěma účelům:

1. Simulací aktivity na připojení je méně pravděpodobné, že by síť síťové vrstvy, která je zodpovědná za uzavření neaktivních připojení, vypnula vaše připojení.
2. Je-li připojení ukončeno, je zkráceno zpoždění před tím, než dojde k přerušení nefunkčních připojení.

Výchozí interval udržení aktivity TCP/IP je dvě hodiny. Zvažte nastavení atributů KAIN a HBINT na kratší dobu. Nepředpokládejte, že normální chování sítě vyhovuje potřebám automatického opětovného připojení. Například některé brány firewall mohou vypnout neaktivní připojení TCP/IP po uplynutí pouhých 10 minut.

Síťová konektivita

Pouze selhání sítě, která jsou předávána síti IBM MQ MQI client , jsou obsluhována schopností automatického opětovného připojení klienta.

- Opětovné připojení provedená automaticky přenosem je neviditelná pro IBM MQ.
- Nastavení HBINT pomáhá vypořádat se se selháními sítě, která jsou neviditelná pro produkt IBM MQ.

Správci front a moduly listener produktu IBM MQ

Přepojení klienta se spouští selháním serveru, selháním správce front, selháním síťového připojení a přepojením administrátora na jinou instanci správce front.

- Pokud používáte správce front s více instancemi, vyskytne se při přepnutí řízení z aktivní instance správce front na instanci v pohotovostním režimu další příčina opakovaného připojení klienta.
- Ukončení správce front s použitím výchozího příkazu **endmqm** nespouští automatické opětovné připojení klienta. Přidejte volbu **-r** do příkazu **endmqm** , chcete-li požádat o automatické opětovné připojení klienta, nebo volbu **-s** pro přenos na instanci správce front v pohotovostním režimu po jeho ukončení.

Podpora automatického opětovného připojení produktu IBM MQ MQI client

Pokud použijete podporu automatického připojení klienta v produktu IBM MQ MQI client, klientská aplikace se automaticky znovu připojí a pokračuje ve zpracování bez zadání volání MQI MQCONN nebo MQCONNX k opětovnému připojení ke správci front.

- Automatické opětovné připojení klienta se spustí jedním z následujících výskytů:
 - selhání správce front
 - ukončení správce front a uvedení příznaku **-r**, opětovného připojení, volba v příkazu **endmqm**
- Volby produktu MQCONNX MQCNO řídí, zda jste povolili automatické opětovné připojení klienta. Volby jsou popsány v části [Volby opětovného připojení](#).
- Automatické opětovné připojení klienta vydává volání MQI jménem vaší aplikace k obnovení manipulátoru připojení a obslužných rutin k dalším otevřeným objektům, takže váš program může pokračovat v běžném zpracování poté, co zpracoval jakékoli chyby MQI, které měly za následek nefunkční připojení. Viz ["Zotavení automaticky znovu připojeného klienta"](#) na stránce 453.
- Pokud jste pro připojení napsali uživatelský program kanálu, tato uživatelská procedura obdrží tato další volání MQI.
- Můžete registrovat obslužnou rutinu událostí opětovného připojení, která se spustí při zahájení opětovného připojení a kdy skončí.

Ačkoli zamýšlená doba opětovného připojení není delší než minuta, opětovné připojení může trvat déle, protože správce front může mít mnoho prostředků, které lze spravovat. Během této doby může klientská aplikace zadržovat zámky, které nenáleží k prostředkům produktu IBM MQ . Existuje hodnota časového

limitu, kterou můžete nakonfigurovat k omezení doby, po kterou klient čeká na opětovné připojení. Hodnota (v sekundách) je nastavena v souboru `mqclient.ini`.

```
Channels:  
MQReconnectTimeout = 1800
```

Po vypršení časového limitu nejsou provedeny žádné pokusy o opětovné připojení. Když systém zjistí, že časový limit vypršel, vrátí chybu `MQRC_RECONNECT_FAILED`.

Monitorování zpráv konzoly

Existuje řada informačních zpráv vydaných správcem front nebo inicializačním programem kanálu, které mají být považovány za zvláště významné. Tyto zprávy samy o sobě neoznačují problém, ale mohou být užitečné při sledování, protože označují potenciální problém, který může vyžadovat adresování.

Přítomnost těchto zpráv konzoly může také označovat, že uživatelská aplikace vkládá do sady stránek velký počet zpráv, což může být příznakem většího problému:

- Problém s aplikací uživatele, které zprávy PUTs, jako např. neřízená smyčka.
- Uživatelská aplikace, která zÍSKuje zprávy z fronty, již nefunguje.

Zotavení z chyb klastru pro servery na distribuovaných platformách

 distributed

Počínaje produktem IBM WebSphere MQ 7.1 správce front znovu spouští operace, které způsobily problémy, dokud nejsou problémy vyřešeny. Další informace naleznete v tématu [Změny zotavení z chyb klastru na serverech jiných než z/OS](#).

Zprávy konzoly určené k monitorování

 z/OS

Následující seznam popisuje zprávy, které mohou potenciálně znamenat větší problémy. Určete, zda je nezbytné sledovat tyto zprávy se systémovou automatizací a poskytnout příslušnou dokumentaci, aby mohly být všechny potenciální problémy následovány efektivně.

CSQI004I: csect-name SUEL INDEXING *název-fronty* BY *typ_indexu* FOR *typ-připojení* CONNECTION *název-připojení*, počet_zpráv MESSAGES PŘESKOČENO

- Správce front zjistil, že aplikace přijímá zprávy podle ID zprávy nebo ID korelace z fronty, která nemá definovaný index.
- Zvažte vytvoření indexu pro danou frontu změnou lokálního objektu fronty *název-fronty*, atributu `INDXTYPE`, který má hodnotu *typ_indexu*.

CSQI031I: csect-name NEW EXTENT OF PAGE SET *psid* BYL FORMÁTOVANÝ ÚSPĚŠNĚ

- Zkontrolujte hloubku fronty front přidělených k této sadě stránek.
- Vyšetřete příčinu selhání při zpracování zpráv.

CSQI041I: csect-name JOB *jméno úlohy* USER *ID uživatele* HAD ERROR ACCESING PAGE SET *psid*

- Určete, zda je sada stránek přidělena ke správci front.
- Zadejte příkaz `DISPLAY USAGE` k určení stavu sady stránek.
- Zkontrolujte protokol úlohy správce front, zda obsahuje další chybové zprávy.

CSQI045I: csect-name Dosažen protokol RBA protokolu *rba*. Plánování resetování protokolu

- Naplánujte zastavení správce front v příhodném čase a resetujte protokoly.

- Pokud správce front používá 6 bajtů protokolu RBA, zvažte možnost převodu správce front tak, aby používal protokol s 8bajtovými centrály RBA.

CSQI046E: csect-name Dosažen protokol RBA protokolu rba. Provést resetování protokolu

- Naplánujte zastavení správce front v příhodném čase a resetujte protokoly.
- Pokud správce front používá 6 bajtů protokolu RBA, zvažte možnost převodu správce front tak, aby používal protokol s 8bajtovými centrály RBA.

CSQI047E: csect-name Protokol RBA protokolu dosáhl rba. Zastavení správce front a resetování protokolů

- Zastavte správce front okamžitě a resetujte protokoly.
- Pokud správce front používá 6 bajtů protokolu RBA, zvažte možnost převodu správce front tak, aby používal protokol s 8bajtovými centrály RBA.

CSQJ004I: ACTIVE LOG COPY n INACTIVE, LOG IN SINGLE MODE, ENDPBA= ttt

- Správce front aktivoval režim protokolování 'single'. To často svědčí o problému při odkládání protokolu.
- Zadejte příkaz **DISPLAY LOG** k určení nastavení pro oboustranný tisk aktivních a archivních protokolů. Tato obrazovka také ukazuje, kolik aktivních protokolů vyžaduje zpracování odkládání.
- Zkontrolujte protokol úlohy správce front, zda obsahuje další chybové zprávy.

CSQJ031D: csect-name, LOG RBA RANGE MUSÍ BÝT RESET. ODPOVĚĚ 'Y' POKRAČOVAT SPUŠTĚNÍ NEBO ' N' TO SHUTDOWN

- Zastavte správce front a resetujte protokoly, jakmile to bude možné, a resetujte protokoly.
- Pokud správce front používá 6 bajtů protokolu RBA, zvažte možnost převodu správce front tak, aby používal protokol s 8bajtovými centrály RBA.

CSQJ032E: csect-name alert-lvl -APPROACHING END OF THE LOG RBA RANGE OF max-rba. CURRENT LOG RBA IS current-rba.

- Chcete-li správce front zastavit a resetovat protokoly co nejdříve, naplánujte jejich zastavení.
- Pokud správce front používá 6 bajtů protokolu RBA, zvažte možnost převodu správce front tak, aby používal protokol s 8bajtovými centrály RBA.

CSQJ110E: POSLEDNÍ KOPIEn AKTIVNÍ PROTOKOL DAT SET IS nnn PERCENT FULL

- Proveďte kroky k dokončení dalších čekajících úloh odlehčování provedením požadavku na zobrazení, abyste určili nevyřízené požadavky související s procesem odsunutí protokolu. Proveďte nezbytnou akci ke splnění všech požadavků a povolte pokračování odlehčování.
- Zvažte, zda jsou k dispozici dostatek aktivních datových sad protokolů. Je-li to nutné, můžete dynamicky přidávat další datové sady protokolů pomocí příkazu **DEFINE LOG** .

CSQJ111A: MIMO PROSTOR V AKTIVNÍM SOUBORU PROTOKOLU PROTOKOLU

- Proveďte požadavek na zobrazení, abyste se ujistili, že neexistují žádné nevyřízené požadavky, které souvisejí s procesem odsunutí protokolu. Proveďte nezbytnou akci ke splnění všech požadavků a povolte pokračování odlehčování.
- Zvažte, zda jsou k dispozici dostatek aktivních datových sad protokolů. Je-li to nutné, můžete dynamicky přidávat další datové sady protokolů pomocí příkazu **DEFINE LOG** .
- Pokud bylo zpoždění způsobeno nedostatkem prostředků nutným pro odlehčování, musí být k dispozici nezbytný prostředek, aby bylo možné provést odlehčování, a proto povolit pokračování protokolování. Chcete-li získat informace o zotavení z této podmínky, prohlédněte si téma [Problémy s protokolem archivace](#).

CSQJ114I: CHYBA PŘI NASTAVENÍ ARCHIVACE, NABÍDKA POKRAČUJÍCÍHO SE POUZE JEDNOU ARCHIVNÍ DATOVOU DATU SE GENEROVÁNÍM

- Zkontrolujte protokol úlohy správce front, zda obsahuje další chybové zprávy.

- Vytvořte druhou kopii protokolu archivace a ručně aktualizujte sadu BSDS.

CSQJ115E: OFFLOAD SE NEZDAŘILO, NELZE PŘIDĚLIT SOUBOR ARCHIVACE ARCHIVACE

Zkontrolujte informace o chybovém stavu zprávy CSQJ103E nebo CSQJ073E. Opravte podmínku, která způsobila chybu přidělení datové sady, aby se při pokusu o přenesení mohlo provést odlehčování.

CSQJ136I: NELZE PŘIDĚLIT PÁSKU JEDNOTKU PRO SPOJENÍ-ID= xxxx CORRELATION-ID= yyyyyy, m ALLOCATED n POVOLENO

- Zkontrolujte protokol úlohy správce front, zda obsahuje další chybové zprávy.

CSQJ151I: csect-name ERROR READING RBA rrr, CONNECTION-ID= xxxx CORRELATION-ID= yyyyyy REASON CODE= ccc

- Zkontrolujte protokol úlohy správce front, zda obsahuje další zprávy.
- Vydejte příkaz **DISPLAY CONN**, abyste určili, které připojení nepotvrzuje svou aktivitu.
- Ujistěte se, že aplikace může potvrdit své aktualizace.

CSQJ160I: NOVÁŽ BYLA NALEZENA, URID= urid CONNECTION NAME= název

- Zkontrolujte protokol úlohy správce front, zda obsahuje další zprávy.
- Vydejte příkaz **DISPLAY CONN**, abyste určili, které připojení nepotvrzuje svou aktivitu.
- Ujistěte se, že aplikace může potvrdit své aktualizace.

CSQJ161I: UOW NEVYŘEŠENO PO n OFFLOADS, URID= urid CONNECTION NAME= název

- Určete, zda je sada stránek přidělena ke správci front.
- Zadejte příkaz **DISPLAY USAGE** k určení stavu sady stránek.
- Zkontrolujte protokol úlohy správce front, zda obsahuje další zprávy.

CSQP011E: CONNECT ERROR STATUS ret-code FOR PAGE SET psid

- Zkontrolujte hloubku fronty front přidělených k této sadě stránek.
- Prozkoumejte příčinu selhání při zpracování zpráv.

CSQP013I: csect-name NEW EXTENT CREATED FOR PAGE SET psid. NOVÝ ROZSAH BUDOU ZPŘÍKON

- Zkontrolujte hloubku fronty front přidělených k této sadě stránek.
- Prozkoumejte příčinu selhání při zpracování zpráv.
- Určete, zda je třeba fronty přesunout do jiné sady stránek.
- Je-li nosič plný, určete, zda je třeba nastavit datovou sadu na více svazcích. Je-li sada stránek již více svazků, zvažte přidání více svazků do používané skupiny úložišť. Jakmile je k dispozici více volného místa, zopakujte rozšíření nastavením metody **EXPAND** na hodnotu **SYSTEM**. Je-li požadován nový pokus, přepněte **EXPAND** na **SYSTEM** a pak zpět na normální nastavení.

CSQP014E: csect-name EXPANSION FAILED FOR PAGE SET psid. BUDOUCÍ POŽADAVKY NA ROZŠÍŘENÍ BUDOU ZAMÍTNUTY

- Zkontrolujte hloubku fronty front přidělených k této sadě stránek.
- Prozkoumejte příčinu selhání při zpracování zpráv.
- Určete, zda je třeba fronty přesunout do jiné sady stránek.

CSQP016E: csect-name PAGE SET psid BYL DOSAŽEN MAXIMÁLNÍ POČET EXTENTŮ. IT NELZE ROZŠÍŘIT AGAIN

- Zkontrolujte hloubku fronty front přidělených k této sadě stránek.
- Prozkoumejte příčinu selhání při zpracování zpráv.

CSQP017I: csect-name EXPANSION STARTED FOR PAGE SET psid

Vydejte příkazy **DISPLAY THREAD**, abyste určili stav jednotek práce v produktu IBM MQ.

CSQP047E: Nedostupné sady stránek mohou způsobit problémy-provést akci pro nápravu této situace

- Postupujte podle odezvy systémového programátora.

CSQQ008I: nn jednotek zotavení jsou stále v nejistém stavu ve správci front qqqq

- Prozkoumejte stav fronty nedoručených zpráv. Ujistěte se, že fronta nedoručených zpráv není PUT zakázána.
- Ujistěte se, že fronta nedoručených zpráv není v limitu MAXMSG.

CSQQ113I: psb-název id-oblasti Tato zpráva nemůže být zpracována

- Zkontrolujte datovou sadu CSQOUTX, abyste určili příčinu selhání CSQINPX.
- Některé příkazy možná nebudou zpracovány.

CSQX035I: csect-name Připojení ke správci front název_správce_front zastavení nebo přerušování, MQCC= mqcc MQRC= mqrc (mqrc-text)

- Zkontrolujte MQRC, abyste určili příčinu selhání.
- Tyto kódy jsou dokumentovány v příručce IBM MQ for z/OS zpráv, completion, and reason codes.

CSQX032I: csect-name Obslužná rutina příkazu inicializace byla ukončena

- Zkontrolujte MQRC, abyste určili příčinu selhání.
- Tyto kódy jsou dokumentovány v příručce IBM MQ for z/OS zpráv, completion, and reason codes.

CSQX048I: csect-name Nelze převést zprávu pro name, MQCC= mqcc MQRC= mqrc (mqrc-text)

- Zkontrolujte protokol úlohy, abyste určili příčinu selhání TCP/IP.
- Prověřte, zda v adresovém prostoru TCP/IP nejsou chyby.

CSQX234I: Modul listener csect-name byl zastaven, TRPTYPE= trptype INDISP= dispozice

- Pokud se modul listener po příkazu **STOP** nezastaví, zkontrolujte, zda v adresovém prostoru TCP/IP nejsou chyby.
- Postupujte podle odezvy programátora systémů.

CSQX407I: csect-name Fronta klastru q-name definice nekonzistentní

- Více front klastru v rámci klastru má nekonzistentní hodnoty. Vyšetřete a vyřešte rozdíly.

CSQX411I: csect-name Správce úložiště zastaven

- Pokud se správce úložiště zastavil kvůli chybě, zkontrolujte zprávy v protokolu úlohy.

CSQX417I: csect-name Odebratelé klastru zůstanou pro odebraného správce front qmgr-název .

- Postupujte podle odezvy systémového programátora.

CSQX418I: csect-name Pouze jedno úložiště pro klastr název-klastru

- Chcete-li zvýšit vysokou dostupnost, klastry by měly být nakonfigurovány se dvěma úplnými úložišti.

CSQX419I: csect-name Žádné žurnálové zásobníky pro klastr název-klastru

- Postupujte podle odezvy systémového programátora.

CSQX420I: csect-name Žádná úložiště pro klastr cluster-name

- Postupujte podle odezvy systémového programátora.

CSQX448E: csect-name Správce úložiště se zastavil kvůli chybám. Restartovat v n sekundách

- Postupujte podle odezvy systémového programátora.

Tato zpráva se zobrazuje každých 600 sekund (10 minut) až do SYSTEM.CLUSTER.COMMAND.QUEUE je povolena pomocí příkazu:


```
ALTER QLOCAL (SYSTEM.CLUSTER.COMMAND.QUEUE) GET (ENABLED)
```

Před povolením fronty může být zapotřebí ruční intervence k vyřešení problému, který způsobil ukončení správce úložiště, před první zprávou CSQX448E, která se vydává.

Použití produktu IBM MQ s konfiguracemi vysoké dostupnosti

Chcete-li provozovat správce front produktu IBM MQ v konfiguraci vysoké dostupnosti (HA), můžete nastavit správce front tak, aby pracoval buď se správcem funkce vysoké dostupnosti, například PowerHA for AIX (dříve HACMP), nebo Microsoft Cluster Service (MSCS) nebo se správcem front IBM MQ s více instancemi.

Je třeba, abyste si byli vědomi následujících definic konfigurace:

Klastry správců front

Skupiny dvou nebo více správců front na jednom nebo více počítačích, poskytují automatické propojení a umožňují sdílení front mezi nimi pro vyrovnávání zátěže a redundanci.

Klastry HA

Klastry s vysokou dostupností jsou skupiny dvou nebo více počítačů a prostředků, jako jsou disky a sítě, propojené a nakonfigurované takovým způsobem, že pokud dojde k selhání, správce funkce vysoké dostupnosti, jako například HACMP (UNIX) nebo MSCS (Windows) provádí *přepnutí při selhání*. Překonání selhání přenesou stavová data aplikací ze selhávajícího počítače na jiný počítač v klastru a znovu iniciuje jejich činnost. Poskytuje vysokou dostupnost služeb spuštěných v klastru s vysokou dostupností. Vztah mezi klastry produktu IBM MQ a klastry HA je popsán v tématu [“Vztah klastrů s vysokou dostupností do klastrů správců front”](#) na stránce 376.

Správci front s více instancemi

Instance stejného správce front konfigurované ve dvou nebo více počítačích. Spouští se více instancí, jedna instance se stane aktivní instancí a ostatní instance se stanou standbys. Dojde-li k selhání aktivní instance, automaticky převezme rezervní instanci běžící na jiném počítači. Pomocí správců front s více instancemi můžete nakonfigurovat své vlastní vysoce dostupné systémy zasilání zpráv založené na produktu IBM MQ bez nutnosti použití klastrové technologie, jako je HACMP nebo MSCS. Klastry s vysokou dostupností a správci front s více instancemi jsou alternativní způsoby, jak správci front zpřístupnit vysokou dostupnost. Nekombinujte je umístěním správce front s více instancemi do klastru s vysokou dostupností.

Rozdíly mezi správci front s více instancemi a klastry HA

Správci front s více instancemi a klastry s vysokou dostupností jsou alternativní způsoby, jak dosáhnout vysoké dostupnosti pro správce front. Zde jsou některé body, které zdůrazňují rozdíly mezi oběma přístupy.

Správci front s více instancemi zahrnují následující funkce:

- Základní podpora překonání selhání integrovaná do produktu IBM MQ
- Rychlejší překonání selhání než klastr HA
- Jednoduchá konfigurace a operace
- Integrace s produktem MQ Explorer

Omezení správců front s více instancemi zahrnují:

- jsou k dispozici vysoce výkonné síťové úložiště, které je k dispozici
- Složitější konfigurace sítě, protože správce front změní IP adresu, když selže

Klastry HA zahrnují následující funkce:

- Schopnost koordinovat více prostředků, jako je například aplikační server nebo databáze.
- Flexibilnější možnosti konfigurace včetně klastrů zahrnujících více než dva uzly.
- Může překonávání selhání bez zásahu operátora bez obsluhy.
- Převzetí adresy IP správce front jako součásti překonání selhání

Omezení klastrů HA zahrnuje:

- Je třeba zakoupit další nákup produktů a dovednosti.
- Disky, které lze přepínat mezi uzly klastru, jsou povinné.
- Konfigurace klastrů HA je relativně složitá
- Překonání selhání je historicky poměrně pomalé, ale nedávné produkty klastru HA se zlepšují.
- Nepotřebné překonání selhání se mohou vyskytnout, pokud existují nedostatky ve skriptech, které se používají k monitorování prostředků, jako jsou správci front.

Vztah klastrů s vysokou dostupností do klastrů správců front

Klastry správců front poskytují vyrovnávání zátěže zpráv mezi dostupnými instancemi front klastru správce front. Tato nabídka nabízí vyšší dostupnost než jeden správce front, protože po selhání správce front mohou aplikace systému zpráv i nadále odesílat zprávy a přistupovat k přeživovým instancím fronty klastru správce front. Ačkoli však klastry správců front automaticky přesměrují nové zprávy do dostupných správců front v klastru, zprávy aktuálně zařazené do nedostupného správce front nebudou k dispozici, dokud nebude správce front restartován. Z tohoto důvodu samy klastry správců front neposkytují vysokou dostupnost všech dat zpráv nebo poskytují automatickou detekci selhání správce front a automatické spouštění restartování správce front nebo překonání selhání. Klastry vysoké dostupnosti (HA) poskytují tyto funkce. Tyto dva typy klastrů lze použít společně s dobrým účinkem. Úvod do klastrů správců front naleznete v tématu [Navrhování klastrů](#).

Použití produktu IBM MQ s klastrem s vysokou dostupností v systému SYSTÉM UNIX a Linux

Můžete použít produkt IBM MQ s klastrem s vysokou dostupností (HA) na platformách SYSTÉM UNIX a Linux, například PowerHA pro AIX (dříve HACMP), Veritas Cluster Server, HP Serviceguard nebo klastr Red Hat Enterprise Linux s Red Hat Cluster Suite.

Před IBM WebSphere MQ 7.0.1 byl poskytnut produkt SupportPac MC91, který vám pomůže při konfiguraci klastrů HA. Produkt IBM WebSphere MQ 7.0.1 poskytl vyšší stupeň kontroly než předchozí verze, kdy správci front ukládají svá data. Díky tomu je snazší konfigurovat správce front v klastru s vysokou dostupností. Většina skriptů poskytnutých s produktem SupportPac MC91 již není vyžadována a balík SupportPac je stažen.

Tento oddíl představuje [“Konfigurace klastru vysoké dostupnosti”](#) na stránce 376, [vztah klastrů s vysokou dostupností do klastrů správců front](#), [“IBM MQ klienti”](#) na stránce 377a [“IBM MQ pracující v klastru s vysokou dostupností”](#) na stránce 377, a vás provede jednotlivými kroky a poskytuje ukázkové skripty, které můžete upravit, chcete-li nakonfigurovat správce front s klastrem s vysokou dostupností.

V dokumentaci ke klastru s vysokou dostupností se podívejte do dokumentace ke konfiguraci klastru popsaného v této části týkající se vašeho prostředí pro spolupráci s vysokou dostupností.

Konfigurace klastru vysoké dostupnosti

V tomto oddílu je výraz *uzel* použit jako odkaz na entitu, na které běží operační systém a software HA; "počítač", "systém" nebo "počítač" nebo "logická oblast" nebo "blade" mohou být považovány za synonyma v tomto použití. Produkt IBM MQ můžete použít k nastavení buď záložních nebo přejímacích konfigurací, včetně vzájemného převzetí, kde všechny uzly klastru pracují se IBM MQ pracovní zátěží.

Konfigurace *rezervní databáze* je nejzákladnější konfigurací klastru vysoké dostupnosti, v níž jeden uzel provádí práci, zatímco druhý uzel funguje pouze jako rezervní. Záložní uzel neprovedl práci a je označen jako nečinný; tato konfigurace se někdy nazývá *studený pohotovostní režim*. Taková konfigurace vyžaduje vysoký stupeň redundance hardwaru. Chcete-li šetřit na hardwaru, je možné rozšířit tuto konfiguraci tak, aby měla více pracovních uzlů s jedním rezervním uzlem. Poukazuje na to, že záložní uzel může převzít práci všech ostatních pracovních uzlů. Tato konfigurace je stále označována jako záložní konfigurace a někdy také jako konfigurace "N+1".

Převzetí konfigurace je pokročilejší konfigurací, v níž všechny uzly provádějí určitou práci a v případě selhání uzlu je možné převzít práci v rámci kritického zpracování.

Konfigurace *jednostranného převzetí* je jedna z nich, v níž záložní uzel provádí některé další, nekritické a nepřenositelné práce. Tato konfigurace je podobná konfiguraci rezervní databáze, ale s (nekritickou) prací prováděnou záložním uzlem.

Konfigurace *mutual takeover* je ta, ve které všechny uzly provádějí vysoce dostupné (pohyblivé) práce. Tento typ konfigurace klastru s vysokou dostupností je někdy také označován jako "Aktivní/Aktivní", což znamená, že všechny uzly aktivně zpracovávají kritickou pracovní zátěž.

S rozšířenou rezervní konfigurací nebo některou z konfigurací převzetí je důležité zvážit maximální zatížení, které může být umístěno na uzlu, který může převzít práci jiných uzlů. Takový uzel musí mít dostatečnou kapacitu, aby udržel přijatelnou úroveň výkonu.

Vztah klastrů s vysokou dostupností do klastrů správců front

Klastry správců front snižují administraci a poskytují vyrovnávání zátěže zpráv v rámci instancí front klastru správce front. Nabízejí také vyšší dostupnost než jeden správce front, protože po selhání správce front mohou aplikace systému zpráv i nadále přistupovat k přeživším ve frontě klastru správce front. Samotné klastry správců front však neposkytují automatickou detekci selhání správce front a automatické spouštění restartování správce front nebo překonání selhání. Klastry vysoké dostupnosti poskytují tyto funkce. Tyto dva typy klastrů lze použít společně s dobrým účinkem.

IBM MQ klienti

Klienti IBM MQ, kteří komunikují se správcem front, který může být předmětem restartování nebo převzetí, musí být napsány tak, aby tolerovali přerušené připojení a opakovaně se musí pokusit o připojení znovu. Produkt IBM WebSphere MQ verze 7 představil funkce ve zpracování tabulky CCDT (Client Channel Definition Table), které pomáhají s dostupností připojení a vyvážením pracovní zátěže. Tyto funkce však nejsou přímo relevantní při práci se systémem překonání selhání.

Transakční funkčnost umožňuje produktu IBM MQ MQI klient podílet se na dvoudřákových transakcích, pokud je klient připojen ke stejnému správci front. Transakční funkčnost nemůže použít techniky, jako např. prostředek pro rozložení zátěže IP, vybírat ze seznamu správců front. Pokud používáte produkt HA, udržuje správce front svou identitu (název a adresa), na kterémkoliv uzlu běží, takže transakční funkčnost může být použita se správcem front, kteří jsou pod kontrolou funkce HA.

IBM MQ pracující v klastru s vysokou dostupností

Všechny klastry HA mají koncept jednotky překonání selhání. Jedná se o sadu definic, které obsahují všechny prostředky, které tvoří vysoce dostupnou službu. Jednotka překonání selhání zahrnuje samotnou službu a všechny ostatní prostředky, na kterých závisí.

Řešení vysoké dostupnosti používají odlišné podmínky pro jednotku překonání selhání:

- V systémech PowerHA for AIX se jednotka překonání selhání nazývá *skupina prostředků*.
- Na serveru Veritas Cluster Server je znám jako *skupina služeb*.
- Na Serviceguard se nazývá *balík*.

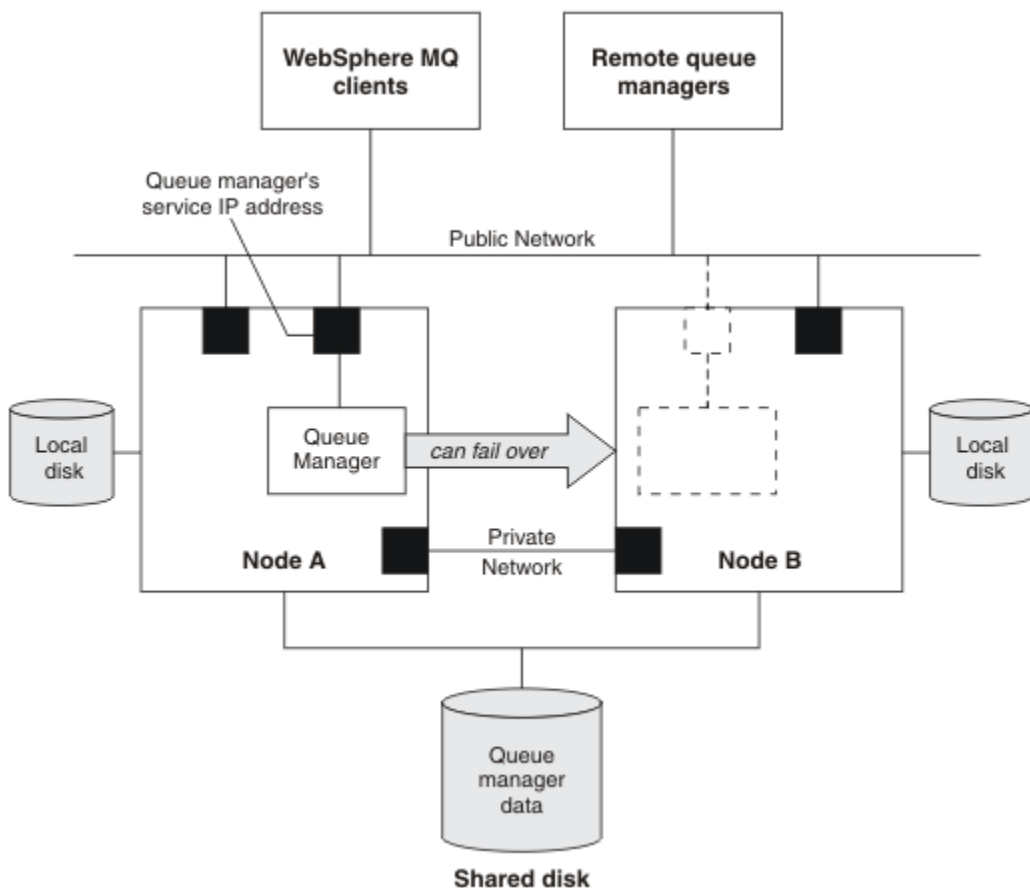
Toto téma používá termín *skupina prostředků* k označení jednotky překonání selhání.

Nejmenší jednotka překonání selhání pro produkt IBM MQ je správce front. Obvykle skupina prostředků obsahující správce front také obsahuje sdílené disky ve skupině svazků nebo ve skupině disků, které jsou vyhrazeny výhradně pro použití skupinou prostředků, a dále adresa IP, která se používá pro připojení ke správci front. Je také možné zahrnout jiné prostředky produktu IBM MQ, jako např. modul listener nebo monitor spouštěčů ve stejné skupině prostředků, buď jako samostatné prostředky, nebo pod řízením správce front jako takového.

Správce front, který má být použit v klastru s vysokou dostupností, musí mít svá data a protokoly na discích, které jsou sdíleny mezi uzly v klastru. Klaster HA zajišťuje, že v daném okamžiku může zapisovat

na disky pouze jeden uzel v klastru. Klastř s vysokou dostupností může ke sledování stavu správce front použít skript monitoru.

Je možné použít jeden sdílený disk jak pro data, tak pro protokoly, které souvisejí se správcem front. Je však běžnou praxí používat samostatné sdílené systémy souborů tak, aby mohly být nezávisle dimenzovány a vyladěny.



Obrázek 71. Klastř vysoké dostupnosti

Obrázek 1 ilustruje klastř s vysokou dostupností se dvěma uzly. Klastř vysoké dostupnosti spravuje dostupnost správce front, který byl definován ve skupině prostředků. Jedná se o aktivní/pasivní nebo studenou záložní konfiguraci, protože pouze jeden uzel, uzel A, momentálně spouští správce front. Správce front byl vytvořen se svými daty a soubory protokolu na sdíleném disku. Správce front má adresu IP služby, která je spravována také klastřem HA. Správce front závisí na sdíleném disku a na jeho adrese IP služby. Selže-li klastř vysoké dostupnosti správce front z uzlu A do uzlu B, přesune nejprve na uzel B závislé prostředky správce front a poté spustí správce front.

Pokud klastř s vysokou dostupností obsahuje více než jednoho správce front, může konfigurace klastřu s vysokou dostupností vést ke spuštění dvou nebo více správců front spuštěných ve stejném uzlu po překonání selhání. Každému správci front v klastřu s vysokou dostupností musí být přiřazeno vlastní číslo portu, které používá v libovolném uzlu klastřu, který má být aktivní v libovolném konkrétním čase.

Obecně je klastř vysoké dostupnosti spuštěn jako uživatel root. Produkt IBM MQ se spouští jako uživatel mqm. Administrace produktu IBM MQ je poskytována členům skupiny mqm. Ujistěte se, že uživatel mqm a skupina existují na všech uzlech klastřu vysoké dostupnosti. ID uživatele a ID skupiny musí být konzistentní v rámci klastřu. Administrace produktu IBM MQ uživatelem root není povolena; skripty, které spouštějí, zastavují nebo monitorují skripty, se musí přepnout na uživatele mqm.

Poznámka: Produkt IBM MQ musí být instalován správně na všech uzlech; nelze sdílet spustitelné soubory produktu.

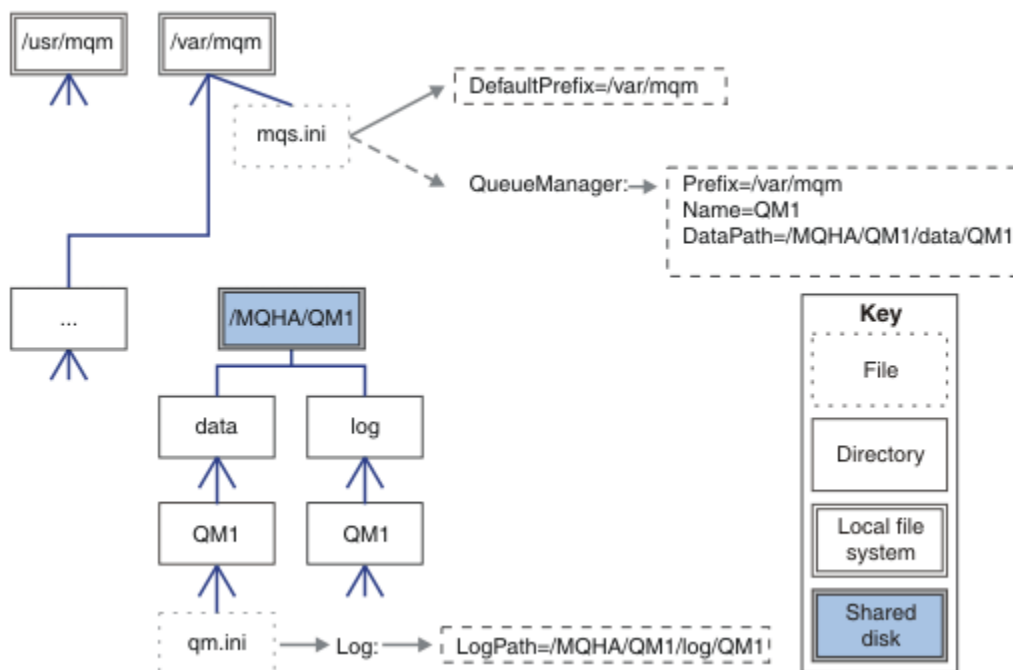
Konfigurace sdílených disků

Správce front IBM MQ v klastru s vysokou dostupností vyžaduje, aby datové soubory a soubory protokolu byly ve společném pojmenovaném vzdáleném systému souborů na sdíleném disku.

Chcete-li konfigurovat sdílené disky, proveďte následující kroky:

1. Rozhodněte se pro názvy bodů připojení pro systémy souborů správce front. Například, /MQHA/qmgrname/data pro datové soubory správce front a /MQHA/qmgrname/log pro své soubory protokolu.
2. Vytvořte skupinu disků (nebo skupinu disků), která bude obsahovat data a soubory protokolu správce front. Tato skupina disků je spravována klastrem vysoké dostupnosti (HA) ve stejné skupině prostředků jako správce front.
3. Vytvořte systémy souborů pro data správce front a soubory protokolu ve skupině svazků.
4. Pro každý uzel dále vytvořte body připojení pro systémy souborů a ujistěte se, že je možné připojit systémy souborů. Uživatel mqm musí vlastnit body připojení.

Obrázek 1 znázorňuje možné rozvržení pro správce front v klastru vysoké dostupnosti. Data a adresáře protokolů správce front jsou umístěny na sdíleném disku, který je připojen v adresáři /MQHA/QM1. Tento disk je přepnut mezi uzly klastru s vysokou dostupností, pokud dojde k překonání selhání, aby byla data dostupná všude, kde je správce front restartován. Soubor mqs.ini obsahuje sekci pro správce front QM1. Sekce Protokol v souboru qm.ini má hodnotu pro LogPath.



Obrázek 72. Sdíleno s názvy adresářů data a log

Vytvoření správce front pro použití v klastru s vysokou dostupností (HA)

Prvním krokem směrem k použití správce front v klastru s vysokou dostupností je vytvoření správce front v jednom z těchto uzlů.

Chcete-li vytvořit správce front pro použití v klastru s vysokou dostupností, vyberte jeden z uzlů v klastru, v němž má být vytvořen správce front. Na tomto uzlu proveďte následující kroky:

1. Připojte systémy souborů správce front v daném uzlu.
2. Vytvořte správce front pomocí příkazu **crtmqm**. Příklad:

```
crtmqm -md /MQHA/qmgrname/data -ld /MQHA/qmgrname/log qmgrname
```
3. Spusťte správce front ručně pomocí příkazu **strmqm**.

4. Dokončete veškeré počáteční konfigurace správce front, jako je například vytváření front a kanálů, a nastavení správce front tak, aby se modul listener spustil automaticky při spuštění správce front.
5. Zastavte správce front pomocí příkazu **endmqm**.
6. Použijte příkaz **dspmqlnf** k zobrazení příkazu **addmqinf**, který můžete použít v pozdější úloze, která je dokumentována v publikaci “Přidání konfiguračních informací správce front do jiných uzlů v klastru s vysokou dostupností (HA)” na stránce 380:

```
dspmqlnf -o command qmgrname
```

kde qmgrname je název správce front.

7. Zobrazený příkaz **addmqinf** bude podobný následujícímu příkladu:

```
addmqinf -sQueueManager -vName=qmgrname -vDirectory=qmgrname \  
-vPrefix=/var/mqm -vDataPath=/MQHA/qmgrname/data/qmgrname
```

Pečlivě si všimněte zobrazeného příkazu.

8. Odpojte systémy souborů správce front.

Nyní jste připraveni dokončit kroky popsané v tématu “Přidání konfiguračních informací správce front do jiných uzlů v klastru s vysokou dostupností (HA)” na stránce 380.

Přidání konfiguračních informací správce front do jiných uzlů v klastru s vysokou dostupností (HA)

Je třeba přidat konfiguraci správce front do ostatních uzlů v klastru s vysokou dostupností.

Před provedením této úlohy musíte provést kroky uvedené v tématu “Vytvoření správce front pro použití v klastru s vysokou dostupností (HA)” na stránce 379.

Chcete-li přidat informace o konfiguraci správce front do každého z ostatních uzlů v klastru s vysokou dostupností, proveďte na každém z dalších uzlů následující kroky:

1. Připojte systémy souborů správce front.
2. Přidejte informace o konfiguraci správce front do uzlu buď přímo úpravou produktu /var/mqm/mqs.ini, nebo zadáním příkazu **addmqinf**, který byl zobrazen pomocí příkazu **dspmqlnf** v krocích 6 a 7 v části “Vytvoření správce front pro použití v klastru s vysokou dostupností (HA)” na stránce 379.
3. Spuštěním a zastavením správce front ověřte konfiguraci.

Příkazy použité ke spuštění a zastavení správce front musí být zadány ze stejné instalace IBM MQ jako příkaz **addmqinf**. Chcete-li spustit a zastavit správce front z jiné instalace, je třeba nejprve nastavit instalaci přidruženou ke správci front pomocí příkazu **setmqm**. Další informace viz [setmqm](#).

4. Odpojte systémy souborů správce front.

Spuštění správce front pod kontrolou klastru s vysokou dostupností (HA)

Správce front je reprezentován v klastru vysoké dostupnosti jako prostředek. Klastr s vysokou dostupností musí být schopen spustit a zastavit správce front. Ve většině případů můžete ke spuštění správce front použít skript shellu. Tyto skripty musíte zpřístupnit ve stejném umístění na všech uzlech v klastru, a to buď pomocí síťového systému souborů, nebo jejich zkopírováním na každý z lokálních disků.

Poznámka: Před restartováním správce front, který selhal, je třeba odpojit vaše aplikace od této instance správce front. Pokud tomu tak není, nemusí se správce front restartovat správně.

Zde jsou uvedeny příklady vhodných skriptů shellu. Tyto vlastnosti můžete upravit podle svých potřeb a použít je ke spuštění správce front pod kontrolou klastru s vysokou dostupností.

Následující skript shellu je příkladem, jak přepnout z uživatele klastru s vysokou dostupností na uživatele mqm, aby mohl být správce front úspěšně spuštěn:

```
#!/bin/ksh  
  
# A simple wrapper script to switch to the mqm user.
```

```
su mqm -c name_of_your_script $*
```

Následující skript shellu je příkladem toho, jak spustit správce front bez jakýchkoli předpokladů týkajících se aktuálního stavu správce front. Všimněte si, že používá extrémně náhlý způsob ukončení všech procesů, které patří ke správci front:

```
#!/bin/ksh
#
# This script robustly starts the queue manager.
#
# The script must be run by the mqm user.

# The only argument is the queue manager name. Save it as QM variable
QM=$1

if [ -z "$QM" ]
then
    echo "ERROR! No queue manager name supplied"
    exit 1
fi

# End any queue manager processes which might be running.

srchstr="( |-m)$QM *.*$"
for process in amqzmuc0 amqzma0 amqfcxba amqfcpub amqpcsea amqzlaa0 \
               amqzlsa0 runmqchi runmqslr amqcrsta amqirmfa amqrmppa \
               amqzfuma amqmuf0 amqzmur0 amqzmgr0
do
    ps -ef | tr "\t" " " | grep $process | grep -v grep | \
    egrep "$srchstr" | awk '{print $2}' | \
    xargs kill -9 > /dev/null 2>&1
done

# It is now safe to start the queue manager.
# The strmqm command does not use the -x flag.
strmqm ${QM}
```

Tento skript můžete upravit tak, aby spouštěl jiné související programy.

Zastavení správce front pod kontrolou klastru s vysokou dostupností (HA)

Ve většině případů můžete ke zastavení správce front použít skript shellu. Zde jsou uvedeny příklady vhodných skriptů shellu. Tyto vlastnosti můžete upravit podle svých potřeb a použít je k zastavení správce front pod kontrolou klastru s vysokou dostupností.

Následující skript je příkladem toho, jak se má okamžitě zastavit, aniž by byly předpoklady o aktuálním stavu správce front uvedeny. Skript musí být spuštěn uživatelem mqm. Proto může být nezbytné zabalit tento skript do skriptu shellu a přepnout uživatele z uživatele klastru s vysokou dostupností do skupiny mqm. (Příklad skriptu shellu je poskytnut v [“Spuštění správce front pod kontrolou klastru s vysokou dostupností \(HA\)”](#) na stránce 380.)

```
#!/bin/ksh
#
# The script ends the QM by using two phases, initially trying an immediate
# end with a time-out and escalating to a forced stop of remaining
# processes.
#
# The script must be run by the mqm user.
#
# There are two arguments: the queue manager name and a timeout value.
QM=$1
TIMEOUT=$2

if [ -z "$QM" ]
then
    echo "ERROR! No queue manager name supplied"
    exit 1
fi

if [ -z "$TIMEOUT" ]
then
    echo "ERROR! No timeout specified"
```

```

    exit 1
fi

for severity in immediate brutal
do
    # End the queue manager in the background to avoid
    # it blocking indefinitely. Run the TIMEOUT timer
    # at the same time to interrupt the attempt, and try a
    # more forceful version. If the brutal version fails,
    # nothing more can be done here.

    echo "Attempting ${severity} end of queue manager '${QM}'"
    case $severity in

    immediate)
        # Minimum severity of endmqm is immediate which severs connections.
        # HA cluster should not be delayed by clients
        endmqm -i ${QM} &
        ;;

    brutal)
        # This is a forced means of stopping queue manager processes.

        srchstr="( |-m)$QM *.*$"
        for process in amqzmuc0 amqzma0 amqfcxba amqfcpub amqpcsea amqzlaa0 \
            amqzlsa0 runmqchi runmqslr amqcrista amqrrmfa amqrmppa \
            amqzfuma amqzmuf0 amqzmur0 amqzmgr0
        do
            ps -ef | tr "\t" " " | grep $process | grep -v grep | \
                egrep "$srchstr" | awk '{print $2}' | \
                    xargs kill -9 > /dev/null 2>&1
        done

    esac

    TIMED_OUT=yes
    SECONDS=0
    while (( $SECONDS < ${TIMEOUT} ))
    do
        TIMED_OUT=yes
        i=0
        while [ $i -lt 5 ]
        do
            # Check for execution controller termination
            srchstr="( |-m)$QM *.*$"
            cnt=`ps -ef | tr "\t" " " | grep amqzma0 | grep -v grep | \
                egrep "$srchstr" | awk '{print $2}' | wc -l`
            i=`expr $i + 1`
            sleep 1
            if [ $cnt -eq 0 ]
            then
                TIMED_OUT=no
                break
            fi
        done

        if [ ${TIMED_OUT} = "no" ]
        then
            break
        fi

        echo "Waiting for ${severity} end of queue manager '${QM}'"
        sleep 1
    done # timeout loop

    if [ ${TIMED_OUT} = "yes" ]
    then
        continue      # to next level of urgency
    else
        break          # queue manager is ended, job is done
    fi

done # next phase

```

Poznámka: V závislosti na tom, které procesy jsou spuštěny pro specifického správce front, nemusí být seznam procesů správce front zahrnutých do tohoto skriptu buď úplný seznam, nebo může obsahovat více procesů než procesy, které jsou spuštěny pro daného správce front:

```
for process in amqzmuc0 amqzma0 amqfcxba amqfcpub amqpcsea amqzlaa0 \  
              amqzlsa0 runmqchi runmqlsr amqcrista amqirmfa amqimppa \  
              amqzfuma amqmuf0 amqzmur0 amqzmgr0
```

Proces může být zahrnut do nebo vyloučen z tohoto seznamu na základě toho, která funkce je konfigurována a jaké procesy jsou spuštěny pro specifického správce front. Úplný seznam procesů a informace o zastavení procesů ve specifickém pořadí naleznete v tématu [Ruční zastavení správce front v systému UNIX a Linux](#).

Monitorování správce front

Je obvyklé poskytovat způsob, jak klastr vysoké dostupnosti (HA) pravidelně monitorovat stav správce front. Ve většině případů můžete použít skript shellu pro tento případ. Zde jsou uvedeny příklady vhodných skriptů shellu. Tyto skripty můžete upravit podle svých potřeb a použít je k provádění dalších kontrol monitorování specifických pro vaše prostředí.

V produktu IBM WebSphere MQ 7.1 je možné mít více instalací IBM MQ koexistujících na systému. Další informace o více instalacích najdete v tématu [Více instalací](#). Hodláte-li používat skript monitorování přes více instalací, včetně instalací v produktu Verze 7.1 nebo vyšší, budete možná muset provést některé další kroky. Pokud máte primární instalaci, nebo používáte skript s verzemi staršími než Verze 7.1, nemusíte pro použití skriptu zadávat `MQ_INSTALLATION_PATH`. Jinak následující kroky zajišťují, že je `MQ_INSTALLATION_PATH` správně identifikován:

1. Chcete-li identifikovat správné `MQ_INSTALLATION_PATH` pro správce front, použijte příkaz `crtmqenv` z instalace produktu Verze 7.1 :

```
crtmqenv -m qmname
```

Tento příkaz vrací správnou hodnotu `MQ_INSTALLATION_PATH` pro správce front určeného parametrem `qmname`.

2. Spusťte skript monitorování s příslušnými parametry `qmname` a `MQ_INSTALLATION_PATH`.

Poznámka: PowerHA for AIX neposkytuje způsob, jak dodat parametr programu monitorování pro správce front. Musíte vytvořit samostatný monitorovací program pro každého správce front, který bude zapouzdřit název správce front. Zde je příklad skriptu použitého v produktu AIX k zapouzdření názvu správce front:

```
#!/bin/ksh  
su mqm -c name_of_monitoring_script qmname MQ_INSTALLATION_PATH
```

kde `MQ_INSTALLATION_PATH` je nepovinný parametr, který určuje cestu k instalaci produktu IBM MQ, ke které je přidružen správce front `název_správce_front`.

Následující skript není robustní na možnost, že produkt `runmqsc` uvázne. Zpravidla jsou klastry vysoké dostupnosti považovány za selhání a jsou pro tuto možnost samy robustní.

Skript však toleruje, že se správce front nachází ve spuštění stavu. Je to proto, že je běžné, že klastr HA spouští monitorování správce front ihned poté, co jej začal. Některé klastry vysoké dostupnosti rozlišují mezi počáteční fází a spuštěnou fází pro prostředky, ale je třeba nakonfigurovat dobu trvání počáteční fáze. Vzhledem k tomu, že doba potřebná ke spuštění správce front závisí na množství práce, které má provést, je obtížné vybrat maximální dobu, kterou spouští správce front. Vyberete-li příliš nízkou hodnotu, klastr vysoké dostupnosti nesprávně předpokládá, že správce front selhal, když se nespustil. To může mít za následek nekonečnou posloupnost failovers.

Tento skript musí být spuštěn uživatelem `mqm`; může být proto nezbytné zabalit tento skript do skriptu shellu a přepnout uživatele z uživatele klastru s vysokou dostupností do systému `mqm` (příklad skriptu shellu je uveden v produktu [“Spuštění správce front pod kontrolou klastru s vysokou dostupností \(HA\)”](#) na stránce 380):

```
#!/bin/ksh  
#  
# This script tests the operation of the queue manager.
```

```

#
# An exit code is generated by the runmqsc command:
# 0 => Either the queue manager is starting or the queue manager is running and responds.
#     Either is OK.
# >0 => The queue manager is not responding and not starting.
#
# This script must be run by the mqm user.
QM=$1
MQ_INSTALLATION_PATH=$2

if [ -z "$QM" ]
then
echo "ERROR! No queue manager name supplied"
exit 1
fi

if [ -z "$MQ_INSTALLATION_PATH" ]
then
# No path specified, assume system primary install or MQ level < 7.1.0.0
echo "INFO: Using shell default value for MQ_INSTALLATION_PATH"
else
echo "INFO: Prefixing shell PATH variable with $MQ_INSTALLATION_PATH/bin"
PATH=$MQ_INSTALLATION_PATH/bin:$PATH
fi

# Test the operation of the queue manager. Result is 0 on success, non-zero on error.
echo "ping qmgr" | runmqsc ${QM} > /dev/null 2>&1
pingresult=$?

if [ $pingresult -eq 0 ]
then # ping succeeded

echo "Queue manager '${QM}' is responsive"
result=0

else # ping failed

# Don't condemn the queue manager immediately, it might be starting.
srchstr="(|-m)$QM *.*$"
cnt=`ps -ef | tr "\t" " " | grep stirmqm | grep "$srchstr" | grep -v grep \
| awk '{print $2}' | wc -l`
if [ $cnt -gt 0 ]
then
# It appears that the queue manager is still starting up, tolerate
echo "Queue manager '${QM}' is starting"
result=0
else
# There is no sign of the queue manager starting
echo "Queue manager '${QM}' is not responsive"
result=$pingresult
fi
fi

exit $result

```

Vložení správce front pod ovládací prvek klastru s vysokou dostupností (HA)

Správce front je třeba konfigurovat pod kontrolou klastru s vysokou dostupností a s použitím adresy IP správce front a sdílených disků.

Chcete-li definovat skupinu prostředků, která bude obsahovat správce front a všechny její přidružené prostředky, postupujte takto:

1. Vytvořte skupinu prostředků obsahující správce front, svazek nebo skupinu disků správce front a adresu IP správce front. Adresa IP je virtuální adresa IP, nikoli adresa IP počítače.
2. Ověřte, že klastr HA správně přepíná prostředky mezi uzly klastru a je připraven k řízení správce front.

Odstranění správce front z uzlu klastru s vysokou dostupností (HA)

Je možné, že budete chtít odebrat správce front z uzlu, který již není potřebný ke spuštění správce front.

Chcete-li odebrat správce front z uzlu v klastru s vysokou dostupností, proveďte následující kroky:

1. Odeberte uzel z klastru s vysokou dostupností tak, aby se klastr s vysokou dostupností již nepokusil o aktivaci správce front v tomto uzlu.

2. Chcete-li odebrat informace o konfiguraci správce front, použijte následující příkaz **rmvmqinf** :

```
rmvmqinf qmgrname
```

Chcete-li správce front zcela odstranit, použijte příkaz **dltmqm** . Mějte však na paměti, že tato operace zcela odstraní data správce front a soubory protokolu. Pokud jste správce front odstranili, můžete pomocí příkazu **rmvmqinf** odebrat zbývající informace o konfiguraci z ostatních uzlů.

Podpora produktu Microsoft Cluster Service (MSCS)

Zavedení a nastavení serveru MSCS pro podporu překonání selhání virtuálních serverů.

Tyto informace platí pouze pro IBM MQ for Windows .

Služba Microsoft Cluster Service (MSCS) vám umožňuje připojit servery do *klastru*, což poskytuje vyšší dostupnost dat a aplikací a usnadňuje správu systému. MSCS může automaticky zjišťovat a zotavovat se ze selhání serveru nebo aplikací.

MSCS podporuje *překonání selhání virtuálních serverů*, které odpovídají aplikacím, webovým stránkám, tiskovým frontám nebo sdílení souborů (včetně například jejich diskových spindel, souborů a adres IP).

Překonání selhání je proces, při kterém MSCS zjistí selhání v aplikaci na jednom počítači v klastru a ukončí přerušenu aplikaci řádným způsobem, přenesení data o stavu do druhého počítače a znovu iniciuje aplikaci.

Tato sekce představuje klastry klastrů MSCS a popisuje nastavení podpory MSCS v následujících sekcích:

- [“Představení klastrů MSCS” na stránce 385](#)
- [“Nastavení produktu IBM MQ pro klastrování MSCS” na stránce 386](#)

Poté se dozvíte, jak nakonfigurovat produkt IBM MQ pro klastrování MSCS, v následujících sekcích:

- [“Vytvoření správce front pro použití se službou MSCS” na stránce 388](#)
- [“Přesun správce front do úložiště MSCS” na stránce 389](#)
- [“Vložení správce front do ovládacího prvku MSCS” na stránce 390](#)
- [“Odebrání správce front z ovládacího prvku MSCS” na stránce 396](#)

A poté poskytne některé užitečné pokyny k použití prostředí MSCS s produktem IBM MQa obsahuje podrobnosti o obslužných programech podpory prostředí MSCS produktu IBM MQ v následujících sekcích:

- [“Rady a tipy pro použití MSCS” na stránce 397](#)
- [“IBM MQ programy obslužného programu pro podporu MSCS” na stránce 400](#)

Představení klastrů MSCS

Klastry MSCS jsou skupiny dvou nebo více počítačů, které jsou vzájemně propojeny a nakonfigurovány tak, že pokud jeden z nich selže, MSCS provede *přepnutí při selhání*, převede stavová data aplikací ze selhávajícího počítače na jiný počítač v klastru a znovu iniciuje jejich činnost.

[“Použití produktu IBM MQ s konfiguracemi vysoké dostupnosti” na stránce 375](#) obsahuje porovnání mezi klastry MSCS, správci front s více instancemi a klastry IBM MQ .

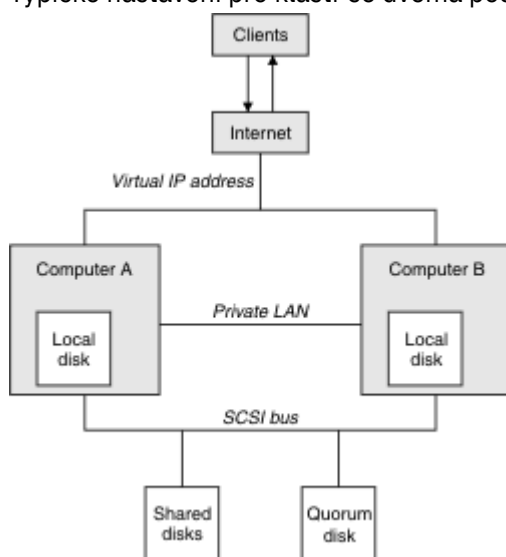
V této sekci a v jejích podřízených tématech výraz *cluster*, je-li používán samostatně, **vždy** znamená klastr MSCS. To je odlišné od klastru IBM MQ popsáno jinde v této příručce.

Klastr se dvěma počítači se skládá ze dvou počítačů (například A a B), které jsou společně připojeny k síti pro klientský přístup pomocí *virtuální IP adresy*. Mohou být také vzájemně propojeny pomocí jedné nebo více soukromých sítí. A a B sdílí alespoň jeden disk pro serverovou aplikaci na každé z nich. Je zde také další sdílený disk, který musí být redundantním polem nezávislých disků (*RAID*). Úroveň 1, pro výlučné použití MSCS; je to známo jako *kvorum* disk. MSCS monitoruje oba počítače, aby kontrolovalo, zda je hardware a software správně spuštěný.

V jednoduchém nastavení, jako je tento, mají oba počítače nainstalovány všechny aplikace, ale pouze počítač A běží s aktivními aplikacemi; počítač B je právě spuštěný a čeká. Pokud počítač A narazí na některou z řady problémů, služba MSCS ukončí přerušenu aplikaci řádným způsobem, přenesení její

stavová data na druhý počítač a znovu zahájí aplikaci. To je známé jako *překonání selhání*. Aplikace mohou být *informovaná o klastru* tak, aby plně spolupracovaly se službou MSCS a failover facefully.

Typické nastavení pro klastr se dvěma počítači je zobrazeno v části [Obrázek 73 na stránce 386](#).



Obrázek 73. Klastr serverů MSCS se dvěma počítači

Každý počítač má přístup ke sdílenému disku, ale pouze jeden po druhém, pod kontrolou MSCS. V případě překonání selhání přepne služba MSCS přístup k jinému počítači. Samotný sdílený disk je obvykle RAID, ale nemusí být.

Každý počítač je připojen k externí síti pro klientský přístup a každý z nich má IP adresu. Avšak externí klient, komunikující s tímto klastru, si je vědom pouze jedné *virtuální adresy IP* a služba MSCS směřuje provoz IP v rámci klastru odpovídajícím způsobem.

MSCS také provádí svou vlastní komunikaci mezi oběma počítači, a to buď prostřednictvím jednoho nebo více soukromých připojení, nebo přes veřejnou síť, například k monitorování stavů pomocí prezenčního signálu a k synchronizaci svých databází.

Nastavení produktu IBM MQ pro klastrování MSCS

Nakonfigurujte produkt IBM MQ pro klastrování tak, že převedíte správce front na jednotku MSCS (překonání selhání). Definujete správce front jako prostředek pro službu MSCS, který jej pak může monitorovat a přenést jej do jiného počítače v klastru, pokud se vyskytne problém.

Chcete-li nastavit systém pro tento systém, začněte instalací produktu IBM MQ na každém počítači v klastru.

Vzhledem k tomu, že správce front je přidružen k názvu instalace produktu IBM MQ, musí být název instalace produktu IBM MQ na všech počítačích v klastru stejný. Viz téma [Instalace a odinstalace](#).

Samotné správce front musí existovat pouze na počítači, na kterém je vytvoříte. V případě překonání selhání iniciuje služba MSCS správce front v jiném počítači. Správci front však musí mít své soubory protokolu a datové soubory na sdíleném disku klastru, nikoli na lokální jednotce. Máte-li již správce front instalovaný na lokální jednotce, můžete jej migrovat pomocí nástroje poskytnutého s produktem IBM MQ; viz [“Přesun správce front do úložiště MSCS”](#) na stránce 389. Chcete-li vytvořit nové správce front pro použití se službou MSCS, přečtěte si téma [“Vytvoření správce front pro použití se službou MSCS”](#) na stránce 388.

Po instalaci a migraci použijte správce klastru MSCS, který bude produkt MSCS informovat o správcích front, viz [“Vložení správce front do ovládacího prvku MSCS”](#) na stránce 390.

Pokud se rozhodnete odebrat správce front z ovládacího prvku MSCS, použijte proceduru popsanou v tématu [“Odebrání správce front z ovládacího prvku MSCS”](#) na stránce 396.

Symetrie nastavení

Když se aplikace přepne z jednoho uzlu na druhou, musí se chovat stejným způsobem, bez ohledu na uzel. Nejlepším způsobem, jak zajistit, aby se tato prostředí shodovala.

Pokud můžete, nastavte klastr se stejným hardwarem, softwarem operačního systému, softwarem produktu a konfigurací na každém počítači. Zejména zkontrolujte, zda je veškerý požadovaný software nainstalovaný na těchto dvou počítačích identický z hlediska verze, úrovně údržby, SupportPacs, cest a uživatelských procedur a že existuje společný prostor jmen (zabezpečení ochrany dat), jak je popsáno v tématu [“Zabezpečení MSCS”](#) na stránce 387.

Zabezpečení MSCS

Pro úspěšné zabezpečení MSCS postupujte podle těchto pokynů.

Pokyny jsou následující:

- Ujistěte se, že máte identické softwarové instalace na každém počítači v klastru.
- Vytvořte obecný obor názvů (prostředí zabezpečení) v rámci klastru.
- Nastavte uzly členů klastru MSCS na doménu, ve které je účet uživatele, který je *vlastníkem klastru*.
- Vytvořte účty ostatních uživatelů v klastru také doménové účty, aby byly k dispozici na obou uzlech. Je tomu tak automaticky, pokud již máte doménu, a účty vztahující se k IBM MQ jsou účty domény. Pokud v současné době nemáte doménu, zvažte nastavení *minidomény*, která bude určena pro uzly klastru a příslušné účty. Vaším cílem je, aby váš klastr dvou počítačů vypadá jako jediný výpočetní prostředek.

Pamatujte na to, že účet, který je lokálně na jednom počítači, neexistuje na druhém počítači. I když vytvoříte účet se stejným názvem na druhém počítači, jeho identifikátor zabezpečení (SID) se liší, takže když se vaše aplikace přesune do jiného uzlu, oprávnění na tomto uzlu neexistují.

Během překonání selhání nebo přesunu produkt IBM MQ MSCS zajistí, aby všechny soubory, které obsahují objekty správce front, měly ekvivalentní povolení v cílovém uzlu. Explicitně, kód zkontroluje, že administrátoři a skupiny mqm a účet SYSTEM mají plnou kontrolu, a že pokud měl Everyone přístup pro čtení ke starému uzlu, je toto oprávnění přidáno do cílového uzlu.

K spuštění služby IBM MQ můžete použít účet domény. Ujistěte se, že existuje v lokální skupině mqm na každém počítači v klastru.

Použití více správců front se službou MSCS

Pokud na počítači provozujete více než jednoho správce front, můžete vybrat jedno z těchto nastavení.

Nastavení jsou následující:

- Všichni správci front v jedné skupině. Pokud se v této konfiguraci vyskytne problém s libovolným správcem front, všechny správce front v rámci skupiny překoná selhání na jiný počítač jako skupinu.
- Jednotlivý správce front v každé skupině. Pokud se v této konfiguraci vyskytne problém se správcem front, dojde k selhání na jiném počítači, aniž by to mělo vliv na ostatní správce front.
- Směs prvních dvou nastavení.

Režimy klastru

Existují dva režimy, ve kterých můžete spustit klastrový systém s IBM MQ: Aktivní/pasivní nebo Aktivní/Aktivní.

Poznámka: Používáte-li službu MSCS spolu se serverem Microsoft Transaction Server (COM +), nemůžete používat aktivní/aktivní režim.

Aktivní/pasivní režim

V režimu Aktivní/Pasivní režim má počítač A spuštěnou aplikaci a počítač B je záložní, používá se pouze tehdy, když MSCS zjistí problém.

Tento režim můžete použít pouze s jedním sdíleným diskem, ale pokud jakákoli aplikace způsobí překonání selhání, **všechny** aplikace musí být přeneseny jako skupina (protože přístup ke sdílenému disku může v daném okamžiku přistupovat pouze jeden počítač).

Můžete nakonfigurovat službu MSCS s hodnotou A jako s počítačem *preferováno* . Poté, je-li počítač A opraven nebo vyměněn a znovu pracuje správně, služba MSCS to zjistí a automaticky přepne aplikaci zpět na počítač A.

Pokud provozujete více než jednoho správce front, zvažte možnost samostatného sdílení se sdíleným diskem pro každý správce front. Poté umístíte každého správce front do samostatné skupiny v prostředí MSCS. Tímto způsobem může kterýkoli správce front provést překonání selhání na jiný počítač, aniž by to mělo vliv na ostatní správce front.

Aktivní/aktivní režim

V Aktivním/aktivním režimu mají počítače A a B spuštěné aplikace a skupiny na každém počítači jsou nastaveny tak, aby používaly jiný počítač jako zálohu. Pokud je na počítači A detekováno selhání, MSCS převede stavová data na počítač B a znovu iniciuje aplikaci. počítač B pak provozuje svou vlastní aplikaci a A je.

Pro toto nastavení budete potřebovat alespoň dva sdílené disky. MSCS můžete nakonfigurovat jako upřednostňovaný počítač pro aplikace A a B jako upřednostňovaný počítač pro aplikace B. Po překonání selhání a opravě se každá aplikace automaticky ukončí na svém vlastním počítači.

Pro IBM MQ to znamená, že můžete například spustit dva správce front, jeden na každém z A a B, přičemž každá z nich využívá plnou moc svého vlastního počítače. Po selhání na počítači A se oba správci front spustí na počítači B. To znamená sdílet sílu jednoho počítače se sníženou schopností zpracovávat velká množství dat při rychlosti. Vaše kritické aplikace však budou stále k dispozici, zatímco opravíte a opravíte poruchu na A.

Vytvoření správce front pro použití se službou MSCS

Tento postup zajišťuje, že bude vytvořen nový správce front takovým způsobem, aby byl vhodný pro přípravu a umístění v rámci řízení MSCS.

Začněš tím, že vytvoříte správce front se všemi jeho prostředky na lokální jednotce a poté migrujete soubory protokolu a datové soubory na sdílený disk. (Tuto operaci můžete vrátit zpět.) **Nesnažte se** vytvořit správce front s jeho prostředky na sdílené jednotce.

Správce front pro použití se službou MSCS můžete vytvořit dvěma způsoby: buď z příkazového řádku, nebo v Průzkumníku IBM MQ . Výhodou použití příkazového řádku je to, že správce front je vytvořen *zastaveno* a nastaven na *ruční spuštění*, které je připraveno pro službu MSCS. (Průzkumník IBM MQ automaticky spustí nového správce front a nastaví jej na automatické spuštění po vytvoření. Musíte to změnit.)

Vytvoření správce front z příkazového řádku

Chcete-li vytvořit správce front z příkazového řádku pro použití se službou MSCS, postupujte takto:

1. Ujistěte se, že máte proměnnou prostředí MQSPREFIX nastavenou tak, aby odkazovala na lokální jednotku, například na C:\WebSphere MQ. Pokud změňte toto nastavení, znovu zaveďte systém počítače, aby se při změně došlo k jeho změně. Pokud proměnnou nenastavíte, bude správce front vytvořen ve výchozím adresáři IBM MQ pro správce front.
2. Vytvořte správce front pomocí příkazu **crtmqm** . Chcete-li například vytvořit správce front s názvem `mcs_test` ve výchozím adresáři, použijte:

```
crtmqm mcs_test
```

3. Pokračujte [“Přesun správce front do úložiště MSCS”](#) na stránce 389.

Vytvoření správce front pomocí Průzkumníka IBM MQ

Chcete-li pomocí Průzkumníka IBM MQ vytvořit správce front pro použití se službou MSCS, postupujte takto:

1. Spusťte Průzkumníka IBM MQ z nabídky Start.
2. V pohledu Navigator rozbalte uzly stromu, abyste našli uzel stromu Queue Managers .
3. Klepněte pravým tlačítkem myši na uzel stromu Queue Managers a vyberte New -> Queue Manager . Zobrazí se panel Vytvoření správce front.
4. Dokončete dialogové okno (krok 1) a poté klepněte na volbu Next> .
5. Dokončete dialogové okno (Krok 2) a poté klepněte na volbu Next> .
6. Dokončete dialogové okno (Krok 3) a ujistěte se, že Start Queue Manager a Create Server Connection Channel nejsou vybrány, a pak klepněte na Next> .
7. Dokončete dialogové okno (krok 4) a poté klepněte na tlačítko Finish .
8. Pokračujte [“Přesun správce front do úložiště MSCS”](#) na stránce 389.

Přesun správce front do úložiště MSCS

Tento postup nakonfiguruje existujícího správce front tak, aby byl vhodný pro vložení do řízení MSCS.

Chcete-li toho dosáhnout, přesunete soubory protokolu a datové soubory na sdílené disky a zpřístupníte je ostatním počítačům v případě selhání. Existující správce front může mít například takové cesty, jako například C:\WebSphere MQ\Log\Neprovádět zkuste soubory přesunout ručně; použijte obslužný program dodávaný jako součást podpory MSCS produktu IBM MQ , jak je popsáno v tomto tématu.

Pokud přesouvaná správce front používá připojení SSL a úložiště klíčů SSL se nachází v datovém adresáři správce front na lokálním počítači, bude úložiště klíčů přesunuto spolu se zbytkem správce front na sdílený disk. Při výchozím nastavení je atribut správce front, který určuje umístění úložiště klíčů SSL, SSLKEYR, nastaven na hodnotu `MQ_INSTALLATION_PATH\qmgrs\QMGRNAME\ssl\key`, která se nachází pod datovým adresářem správce front. `MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ . Příkaz `hamvmqm` neupravuje tento atribut správce front. V této situaci je třeba upravit atribut správce front, SSLKEYR, pomocí Průzkumníka IBM MQ nebo příkazu `MQSC ALTER QMGR`, aby ukazoval na nový soubor úložiště klíčů SSL.

Postup je následující:

1. Ukončete činnost správce front a zkontrolujte, zda nedošlo k žádným chybám.
2. Pokud jsou soubory protokolu správce front nebo soubory fronty již uloženy na sdíleném disku, přeskočte zbývající část této procedury a pokračujte přímo na [“Vložení správce front do ovládacího prvku MSCS”](#) na stránce 390.
3. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (viz [“Soubory protokolu správce front”](#) na stránce 399 , proč je to důležité).
4. Pokud již máte vhodný prostředek sdíleného disku, pokračujte krokem 6. Jinak pomocí administrátora klastru MSCS vytvořte prostředek typu *shared disk* s dostatečnou kapacitou pro ukládání souborů protokolu správce front a datových souborů (fronty).
5. Otestujte sdílený disk pomocí administrátora klastru MSCS a přemístěte jej z jednoho uzlu klastru do druhého a znovu jej přesuňte.
6. Ujistěte se, že je sdílený disk online na uzlu klastru, kde jsou soubory protokolu správce front a datové soubory uloženy lokálně.
7. Spusťte obslužný program k přesunutí správce front následujícím způsobem:

```
hamvmqm /m qmname /dd " e: \
IBM MQ " /ld " e: \
IBM MQ \log"
```

nahrazení názvu správce front názvem *qmname*, písmeno jednotky sdíleného disku pro *ea* váš vybraný adresář pro *IBM MQ*. Adresáře se vytvoří, pokud ještě neexistují.

8. Otestujte správce front, abyste se ujistili, že funguje, pomocí Průzkumníka IBM MQ . Příklad:
 - a. Klepněte pravým tlačítkem myši na uzel stromu správce front a poté vyberte volbu Start . Spustí se správce front.

- b. Klepněte pravým tlačítkem myši na uzel stromu Queues a poté vyberte volbu New -> Local Queue . . . a zadejte název fronty.
 - c. Klepněte na tlačítko Finish .
 - d. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Put Test Message Zobrazí se panel Vložit testovací zprávu.
 - e. Zadejte text zprávy, poté klepněte na tlačítko Put Test Message a zavřete panel.
 - f. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Browse Messages Zobrazí se panel Prohlížeč zpráv.
 - g. Ujistěte se, že zpráva je ve frontě, a klepněte na tlačítko Close . Panel Prohlížeč zpráv se zavře.
 - h. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Clear Messages Zprávy ve frontě jsou vymazány.
 - i. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Delete Zobrazí se panel s potvrzením, klepněte na tlačítko OK . Fronta je odstraněna.
 - j. Klepněte pravým tlačítkem myši na uzel stromu správce front a poté vyberte volbu Stop Zobrazí se panel Ukončení správce front.
 - k. Klepněte na tlačítko OK . Správce front je zastaven.
9. Jako administrátor produktu IBM MQ se ujistěte, že je atribut spuštění správce front nastaven na ruční. V Průzkumníku IBM MQ nastavte pole spuštění na hodnotu manual v panelu vlastností správce front.
10. Pokračujte [“Vložení správce front do ovládacího prvku MSCS”](#) na stránce 390.

Vložení správce front do ovládacího prvku MSCS

Úlohy zahrnuté do umístění správce front v rámci řízení MSCS, včetně nezbytných úloh.

Před vložení správce front pod ovládací prvek MSCS

Před vložení správce front v rámci řízení MSCS proveďte následující úlohy:

1. Ujistěte se, že produkt IBM MQ a jeho podpora MSCS jsou instalovány na obou počítačích v klastru a že software na každém počítači je identický, jak je popsáno v [“Nastavení produktu IBM MQ pro klastrování MSCS”](#) na stránce 386.
2. Obslužný program **haregtyp** použijte k registraci IBM MQ jako typu prostředku MSCS na všech uzlech klastru. Další informace naleznete v dokumentu [“IBM MQ programy obslužného programu pro podporu MSCS”](#) na stránce 400 .
3. Pokud jste správce front dosud nevytvořili, přečtěte si téma [“Vytvoření správce front pro použití se službou MSCS”](#) na stránce 388.
4. Pokud jste správce front vytvořili nebo již existuje, ujistěte se, že jste provedli proceduru v produktu [“Přesun správce front do úložiště MSCS”](#) na stránce 389.
5. Zastavte správce front, je-li spuštěný, a to buď pomocí příkazového řádku, nebo pomocí Průzkumníka IBM MQ .
6. Před přechodem na následující procedury produktu Windows v tomto tématu proveďte test operací MSCS sdílených jednotek.

Windows Server 2012

Chcete-li umístit správce front v rámci řízení MSCS na server Windows Server 2012, použijte následující postup:

1. Přihlaste se k počítači uzlu klastru, který je hostitelem správce front, nebo se přihlaste ke vzdálené pracovní stanici jako uživatel s oprávněním k administraci klastru a připojte se k uzlu klastru, který je hostitelem správce front.
2. Spusťte nástroj Správa klastru pro překonání selhání.

3. Klepněte pravým tlačítkem myši na **Správa klastru pro překonání selhání > Připojit klastr ...** k otevření připojení ke klastru.
4. Na rozdíl od schématu skupiny, které se používá v produktu MSCS Cluster Administrator na předchozích verzích produktu Windows, používá nástroj pro správu klastru pro překonání selhání koncepci služeb a aplikací. Konfigurovaná služba nebo aplikace obsahuje všechny prostředky nezbytné pro klastrování jedné aplikace. Správce front v prostředí MSCS lze konfigurovat takto:
 - a. Klepněte pravým tlačítkem myši na klastr a vyberte volbu **Konfigurovat roli** , chcete-li spustit průvodce konfigurací.
 - b. Vyberte volbu **Jiný server** na panelu "Vybrat službu nebo aplikaci".
 - c. Vyberte příslušnou adresu IP jako přístupový bod klienta.
 Tato adresa by měla být nepoužívanou adresou IP, která má být použita klienty a dalšími správci front pro připojení ke správci front *virtual* . Tato adresa IP není normální (statická) adresa uzlu. Jedná se o přidavnou adresu, která je mezi nimi *floats* . Ačkoli služba MSCS zpracovává směřování této adresy, **neověřuje** , zda je adresa dosažitelná.
 - d. Přiřadte úložné zařízení pro výhradní použití správcem front. Toto zařízení musí být vytvořeno jako instance prostředku, než bude možné je přiřadit.
 K ukládání protokolů a souborů fronty můžete použít jednu jednotku, nebo můžete tyto soubory rozdělit na více jednotek. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, se ujistěte, že všechny jednotky použité tímto správcem front jsou pro tohoto správce front výhradní, to znamená, že nic jiného nespoleská na jednotky. Také se ujistěte, že vytváříte instanci prostředku pro každou jednotku, kterou správce front používá.
 Typ prostředku pro jednotku závisí na podpoře SCSI, kterou používáte; podívejte se na instrukce k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte ji ze své aktuální skupiny do té, která byla vytvořena pro správce front.
 Pro každý prostředek jednotky nastavte možné vlastníky na obou uzlech. Nastavit závislé prostředky na žádné.
 - e. Vyberte prostředek **MQSeries MSCS** na panelu "Vybrat typ prostředku".
 - f. Provedte zbývající kroky v průvodci.
5. Před přivedení prostředku do režimu online potřebuje prostředek MSCS produktu MQSeries další konfiguraci:
 - a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'Nová MSCS MQSeries'.
 - b. Klepněte pravým tlačítkem myši na položku **Vlastnosti** v prostředku MQ .
 - c. Konfigurujte prostředek:
 - Name ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
 - Run in a separate Resource Monitor ; pro lepší izolaci
 - Possible owners ; nastavit oba uzly
 - Dependencies ; Přidejte jednotku a adresu IP pro tohoto správce front.

Varování: Selhání při přidávání těchto závislostí znamená, že produkt IBM MQ se pokusí zapsat stav správce front na chybný disk klastru během překonání selhání. Vzhledem k tomu, že se mnoho procesů může pokusit o zápis na tento disk současně, některé procesy IBM MQ mohou být zablokovány ze spuštění.

 - Parameters ; takto:
 - QueueManagerName (povinné); název správce front, kterého má tento prostředek řídit. Tento správce front musí existovat na lokálním počítači.
 - PostOnlineCommand (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz ["Příkaz PostOnlinea příkaz PreOffline"](#) na stránce 399.

- PreOfflineCommand (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu online na offline. Další podrobnosti viz [“Příkaz PostOnlinea příkaz PreOffline”](#) na stránce 399.

Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 60000 ms. Tyto výchozí hodnoty lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz [“Souhrn výzev looksAlive a isAlive”](#) na stránce 396.

- Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu [“Použití preferovaných uzlů”](#) na stránce 400).
 - Zásada pro překonání selhání* je standardně nastavena na citlivé hodnoty, ale můžete vyladit prahové hodnoty a období, které řídí *překonání selhání prostředků* a *Překonání selhání skupiny* tak, aby odpovídaly zavedům umístěným na správci front.
- Otestujte správce front tím, že jej otevřete online v produktu MSCS Cluster Administrator a vystavujete jej testovací pracovní zátěži. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM MQ . Příklad:
 - Klepněte pravým tlačítkem myši na uzel stromu Queues a poté vyberte volbu New -> Local Queue . . . a zadejte název fronty.
 - Klepněte na tlačítko Finish . Fronta se vytvoří a zobrazí se v zobrazení obsahu.
 - Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Put Test Message Zobrazí se panel Vložit testovací zprávu.
 - Zadejte text zprávy, poté klepněte na tlačítko Put Test Message a zavřete panel.
 - Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Browse Messages Zobrazí se panel Prohlížeč zpráv.
 - Ujistěte se, že vaše zpráva je ve frontě, a klepněte na tlačítko Close . Panel Prohlížeč zpráv se zavře.
 - Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Clear Messages Zprávy ve frontě jsou vymazány.
 - Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Delete Zobrazí se panel s potvrzením, klepněte na tlačítko OK . Fronta je odstraněna.
 - Otestujte, zda lze správce front převést do stavu offline a zpět online pomocí administrátora klastru MSCS.
 - Simulovat překonání selhání.

V Administrátorovi klastru MSCS klepněte pravým tlačítkem myši na skupinu obsahující správce front a vyberte volbu Move Group. To může trvat několik minut. (Pokud chcete rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části [“Přesun správce front do úložiště MSCS”](#) na stránce 389.) Můžete také klepnout pravým tlačítkem myši a vybrat Initiate Failure ; Akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows Server 2008

Chcete-li umístit správce front v rámci řízení MSCS na server Windows Server 2008, postupujte takto:

- Přihlaste se k počítači uzlu klastru, který je hostitelem správce front, nebo se přihlaste ke vzdálené pracovní stanici jako uživatel s oprávněním k administraci klastru a připojte se k uzlu klastru, který je hostitelem správce front.
- Spusťte nástroj Správa klastru pro překonání selhání.
- Klepněte pravým tlačítkem myši na **Správa klastru pro překonání selhání > Spravovat klastr ...** k otevření připojení ke klastru.
- Na rozdíl od schématu skupiny, které se používá v produktu MSCS Cluster Administrator na předchozích verzích produktu Windows, používá nástroj pro správu klastru pro překonání selhání koncepci služeb a aplikací. Konfigurovaná služba nebo aplikace obsahuje všechny prostředky nezbytné pro klastrování jedné aplikace. Správce front v prostředí MSCS lze konfigurovat takto:

- a. Klepněte pravým tlačítkem myši na **Služby a aplikace > Konfigurovat službu nebo aplikaci ...** a spusťte průvodce konfigurací.
 - b. Vyberte volbu **Další server** na panelu **Vybrat službu nebo aplikaci** .
 - c. Vyberte příslušnou adresu IP jako přístupový bod klienta.
 Tato adresa by měla být nepoužívanou adresou IP, která má být použita klienty a dalšími správci front pro připojení ke správci front *virtual* . Tato adresa IP není normální (statická) adresa uzlu. Jedná se o přidavnou adresu, která je mezi nimi *floats* . Ačkoli služba MSCS zpracovává směřování této adresy, **neověřuje** , zda je adresa dosažitelná.
 - d. Přiřadte úložné zařízení pro výhradní použití správcem front. Toto zařízení musí být vytvořeno jako instance prostředku, než bude možné je přiřadit.
 K ukládání protokolů a souborů fronty můžete použít jednu jednotku, nebo můžete tyto soubory rozdělit na více jednotek. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, se ujistěte, že všechny jednotky použité tímto správcem front jsou pro tohoto správce front výhradní, to znamená, že nic jiného nespolehá na jednotky. Také se ujistěte, že vytváříte instanci prostředku pro každou jednotku, kterou správce front používá.
 Typ prostředku pro jednotku závisí na podpoře SCSI, kterou používáte; podívejte se na instrukce k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte ji ze své aktuální skupiny do té, která byla vytvořena pro správce front.
 Pro každý prostředek jednotky nastavte možné vlastníky na obou uzlech. Nastavit závislé prostředky na žádné.
 - e. Vyberte prostředek **MQSeries MSCS** na panelu **Výběr typu prostředku** .
 - f. Proveďte zbývající kroky v průvodci.
5. Před přivedení prostředku do režimu online potřebuje prostředek MSCS produktu MQSeries další konfiguraci:
- a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'Nová MSCS MQSeries'.
 - b. Klepněte pravým tlačítkem myši na položku **Vlastnosti** v prostředku MQ .
 - c. Konfigurujte prostředek:
 - Name ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
 - Run in a separate Resource Monitor ; pro lepší izolaci
 - Possible owners ; nastavit oba uzly
 - Dependencies ; Přidejte jednotku a adresu IP pro tohoto správce front.

Varování: Selhání při přidávání těchto závislostí znamená, že produkt IBM MQ se pokusí zapsat stav správce front na chybný disk klastru během překonání selhání. Vzhledem k tomu, že se mnoho procesů může pokusit o zápis na tento disk současně, některé procesy IBM MQ mohou být zablokovány ze spuštění.

 - Parameters ; takto:
 - QueueManagerName (povinné); název správce front, kterého má tento prostředek řídit. Tento správce front musí existovat na lokálním počítači.
 - PostOnlineCommand (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz [“Příkaz PostOnlinea příkaz PreOffline”](#) na stránce 399.
 - PreOfflineCommand (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu online na offline. Další podrobnosti viz [“Příkaz PostOnlinea příkaz PreOffline”](#) na stránce 399.

Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 60000 ms. Tyto výchozí hodnoty lze upravit pouze po

dokončení definice prostředku. Další podrobnosti viz [“Souhrn výzev looksAlive a isAlive”](#) na stránce 396.

- d. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu [“Použití preferovaných uzlů”](#) na stránce 400).
 - e. *Zásada pro překonání selhání* je standardně nastavena na citlivé hodnoty, ale můžete vyladit prahové hodnoty a období, které řídí *překonání selhání prostředků a Překonání selhání skupiny* tak, aby odpovídaly zavedům umístěným na správci front.
6. Otestujte správce front tím, že jej otevřete online v produktu MSCS Cluster Administrator a vystavujete jej testovací pracovní zátěží. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM MQ . Příklad:
- a. Klepněte pravým tlačítkem myši na uzel stromu Queues a poté vyberte volbu New -> Local Queue . . . a zadejte název fronty.
 - b. Klepněte na tlačítko Finish . Fronta se vytvoří a zobrazí se v zobrazení obsahu.
 - c. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Put Test Message Zobrazí se panel **Vložit testovací zprávu** .
 - d. Zadejte text zprávy, poté klepněte na tlačítko Put Test Message a zavřete panel.
 - e. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Browse Messages Zobrazí se panel **Prohlížeč zpráv** .
 - f. Ujistěte se, že vaše zpráva je ve frontě, a klepněte na tlačítko Close . Panel **Prohlížeč zpráv** se zavře.
 - g. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Clear Messages Zprávy ve frontě jsou vymazány.
 - h. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Delete Zobrazí se panel s potvrzením, klepněte na tlačítko OK . Fronta je odstraněna.
7. Otestujte, zda lze správce front převést do stavu offline a zpět online pomocí administrátora klastru MSCS.
8. Simulovat překonání selhání.

V Administrátorovi klastru MSCS klepněte pravým tlačítkem myši na skupinu obsahující správce front a vyberte volbu Move Group. To může trvat několik minut. (Pokud chcete rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části [“Přesun správce front do úložiště MSCS”](#) na stránce 389.) Můžete také klepnout pravým tlačítkem myši a vybrat Initiate Failure ; Akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows 2003

Chcete-li umístit správce front do řízení MSCS na serveru Windows 2003, použijte následující postup:

1. Přihlaste se k počítači uzlu klastru, který je hostitelem správce front, nebo se přihlaste ke vzdálené pracovní stanici jako uživatel s oprávněním k administraci klastru a připojte se k uzlu klastru, který je hostitelem správce front.
2. Spusťte administrátora klastru MSCS.
3. Otevřete připojení ke klastru.
4. Vytvořte skupinu MSCS, která má být použita k uchování prostředků pro správce front. Pojmenujte skupinu takovým způsobem, že je zřejmé, ke kterému správci front se vztahuje. Každá skupina může obsahovat více správců front, jak je popsáno v tématu [“Použití více správců front se službou MSCS”](#) na stránce 387.

Použijte skupinu pro všechny zbývající kroky.

5. Vytvořte instanci prostředku pro každou logickou jednotku SCSI, kterou používá správce front.

K ukládání protokolů a souborů fronty můžete použít jednu jednotku, nebo můžete tyto soubory rozdělit na více jednotek. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, se ujistěte, že všechny jednotky použité tímto správcem front jsou pro tohoto správce front výhradní,

to znamená, že nic jiného nespolehá na jednotky. Také se ujistěte, že vytváříte instanci prostředku pro každou jednotku, kterou správce front používá.

Typ prostředku pro jednotku závisí na podpoře SCSI, kterou používáte; podívejte se na instrukce k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte ji ze své aktuální skupiny do té, která byla vytvořena pro správce front.

Pro každý prostředek jednotky nastavte možné vlastníky na obou uzlech. Nastavit závislé prostředky na žádné.

6. Vytvořte instanci prostředku pro adresu IP.

Vytvořte prostředek adresy IP (typ prostředku *IP adresa*). Tato adresa by měla být nepoužívanou adresou IP, která má být použita klienty a dalšími správci front pro připojení ke správci front *virtual*. Tato adresa IP není normální (statická) adresa uzlu. Jedná se o přídatnou adresu, která je mezi nimi *floats*. Ačkoli služba MSCS zpracovává směrování této adresy, **neověřuje**, zda je adresa dosažitelná.

7. Vytvořte instanci prostředku pro správce front.

Vytvořte prostředek typu *IBM MQ MSCS*. Průvodce vás vyzve k zadání různých položek, včetně následujících:

- Name ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
- Add to group ; použijte skupinu, kterou jste vytvořili
- Run in a separate Resource Monitor ; pro lepší izolaci
- Possible owners ; nastavit oba uzly
- Dependencies ; Přidejte jednotku a adresu IP pro tohoto správce front.

Varování: Selhání při přidávání těchto závislostí znamená, že produkt IBM MQ se pokusí zapsat stav správce front na chybný disk klastru během překonání selhání. Vzhledem k tomu, že se mnoho procesů může pokusit o zápis na tento disk současně, některé procesy IBM MQ mohou být zablokovány ze spuštění.

- Parameters ; takto:
 - QueueManagerName (povinné); název správce front, kterého má tento prostředek řídit. Tento správce front musí existovat na lokálním počítači.
 - PostOnlineCommand (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz [“Příkaz PostOnlinea příkaz PreOffline”](#) na stránce 399.
 - PreOfflineCommand (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu online na offline. Další podrobnosti viz [“Příkaz PostOnlinea příkaz PreOffline”](#) na stránce 399.

Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 30000 ms. Tyto výchozí hodnoty lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz [“Souhrn výzev looksAlive a isAlive”](#) na stránce 396.

8. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu [“Použití preferovaných uzlů”](#) na stránce 400).
9. *Zásada překonání selhání* (definovaná ve vlastnostech skupiny) je standardně nastavena na citlivé hodnoty, ale můžete vyladit prahové hodnoty a období, které řídí *překonání selhání prostředků* a *Překonání selhání skupiny* tak, aby odpovídaly zátěži umístěné ve správci front.
10. Otestujte správce front tím, že jej otevřete online v produktu MSCS Cluster Administrator a vystavujete jej testovací pracovní zátěži. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM MQ. Příklad:
 - a. Klepněte pravým tlačítkem myši na uzel stromu Queues a poté vyberte volbu New -> Local Queue . . . a zadejte název fronty.
 - b. Klepněte na tlačítko Finish . Fronta se vytvoří a zobrazí se v zobrazení obsahu.

- c. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Put Test Message Zobrazí se panel **Vložit testovací zprávu** .
 - d. Zadejte text zprávy, poté klepněte na tlačítko Put Test Message a zavřete panel.
 - e. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Browse Messages Zobrazí se panel **Prohlížeč zpráv** .
 - f. Ujistěte se, že vaše zpráva je ve frontě, a klepněte na tlačítko Close . Panel **Prohlížeč zpráv** se zavře.
 - g. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Clear Messages Zprávy ve frontě jsou vymazány.
 - h. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu Delete Zobrazí se panel s potvrzením, klepněte na tlačítko OK . Fronta je odstraněna.
11. Otestujte, zda lze správce front převést do stavu offline a zpět online pomocí administrátora klastru MSCS.
12. Simulovat překonání selhání.

V Administrátorovi klastru MSCS klepněte pravým tlačítkem myši na skupinu obsahující správce front a vyberte volbu Move Group. To může trvat několik minut. (Pokud chcete rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části [“Přesun správce front do úložiště MSCS”](#) na stránce 389.) Můžete také klepnout pravým tlačítkem myši a vybrat Initiate Failure ; Akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Souhrn výzev looksAlive a isAlive

looksAlive a *isAlive* jsou intervaly, kdy volání MSCS vrací zpět do typů prostředků a požaduje, aby prostředek provedl kontrolu, aby určil vlastní provozní stav. To v konečném důsledku určuje, zda se MSCS pokusí o překonání selhání prostředku.

Při každé příležitosti, kdy vyprší interval *looksAlive* (výchozí 5000 ms), je prostředek správce front volán, aby provedl svou vlastní kontrolu, aby určil, zda je jeho stav uspokojivý.

Při každé příležitosti, kdy vyprší interval *isAlive* (výchozí hodnota 30000 ms), je pro prostředek správce front provedeno další volání k provedení další kontroly, aby bylo možné určit, zda prostředek správně funguje. To umožňuje dvě úrovně kontroly typů prostředků.

1. Kontrola stavu *looksAlive* se má zjistit, zda se prostředek jeví jako funkční.
2. Významnější kontrola *isAlive* , která určuje, zda je prostředek správce front aktivní.

Je-li prostředek správce front určen jako neaktivní, MSCS na základě dalších rozšířených voleb MSCS spustí překonání selhání pro prostředek a přidružené závislé prostředky na jiném uzlu v klastru. Další informace naleznete v tématu [Dokumentace MSCS](#).

Odebrání správce front z ovládacího prvku MSCS

Správce front můžete odebrat z ovládacího prvku MSCS a vrátit je do ruční administrace.

Odebrání správců front z ovládacího prvku MSCS pro operace údržby není nutné. Můžete to provést tak, že správce front MSCS dočasně, a to tak, že použijete administrátora klastru MSCS. Odebrání správce front z řízení MSCS je trvalejší změna. Pouze pokud se rozhodnete, že nechcete, aby MSCS měl další kontrolu nad správcem front, stačí ji již nadále měnit.

Pokud je správce front odebíván pomocí připojení TSL nebo SSL, musíte upravit atribut správce front SSLKEYR pomocí Průzkumníka IBM MQ nebo příkazu MQSC ALTER QMGR, aby ukazoval na soubor úložiště klíčů SSL v lokálním adresáři.

Postup je:

1. Převeďte prostředek správce front do stavu offline pomocí administrátora klastru MSCS, jak je popsáno v tématu [“Převedení správce front do režimu offline z prostředí MSCS”](#) na stránce 397 .
2. Zlikvidovat instanci prostředku. Tím nedojde ke zničení správce front.
3. Volitelně proveďte migraci souborů správce front zpět ze sdílených jednotek na lokální jednotky. Chcete-li to provést, viz [“Vrácení správce front z úložiště MSCS”](#) na stránce 397.

4. Otestujte správce front.

Převedení správce front do režimu offline z prostředí MSCS

Chcete-li správce front převést do stavu offline z prostředí MSCS, proveďte následující kroky:

1. Spusťte administrátora klastru MSCS.
2. Otevřete připojení ke klastru.
3. Vyberte položku *Groups* nebo *Role*, pokud používáte produkt Windows 2012, a otevřete skupinu obsahující správce front, který má být přesunut.
4. Vyberte prostředek správce front.
5. Klepněte na něj pravým tlačítkem myši a vyberte volbu *Offline*.
6. Čekejte na dokončení.

Vrácení správce front z úložiště MSCS

Tento postup nakonfiguruje správce front tak, aby se vrátil zpět na lokální diskovou jednotku počítače, tj. stane se *normálním* správcem front IBM MQ. Chcete-li toho dosáhnout, přesuňte soubory protokolu a datové soubory ze sdílených disků. Existující správce front může mít například takové cesty, jako například `E:\WebSphere MQ\log\<QMname>` a `E:\WebSphere MQ\mqmgs\<QMname>`. Nepokoušejte se soubory přesunout ručně; pomocí obslužného programu **hamvmqm** dodávaného jako součást podpory MSCS produktu IBM MQ postupujte takto:

1. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (viz [“Soubory protokolu správce front” na stránce 399](#), proč je to důležité).
2. Rozhodněte se, kterou lokální jednotku chcete použít, a ujistěte se, že má dostatečnou kapacitu pro ukládání souborů protokolu správce front a datových souborů (fronty).
3. Ujistěte se, že sdílený disk, na kterém jsou momentálně umístěny soubory, je online na uzlu klastru, do kterého se má přesunout protokol správce front a datové soubory.
4. Spusťte obslužný program k přesunutí správce front následujícím způsobem:

```
hamvmqm /m qmname /dd " c:\
IBM MQ " /ld "c:\
IBM MQ \log"
```

nahrazení názvu správce front *qmname*, písmeno vaší lokální diskové jednotky pro ca vámi zvolený adresář pro *IBM MQ* (adresáře jsou vytvořeny, pokud ještě neexistují).

5. Otestujte správce front a ujistěte se, že pracuje (jak je popsáno v tématu [“Přesun správce front do úložiště MSCS” na stránce 389](#)).

Rady a tipy pro použití MSCS

Tento oddíl obsahuje některé obecné informace, které vám pomohou efektivně využívat podporu produktu IBM MQ pro službu MSCS.

Tento oddíl obsahuje některé obecné informace, které vám pomohou efektivně využívat podporu produktu IBM MQ pro službu MSCS.

Jak dlouho trvá, než se správce front nezdaří z jednoho počítače na druhý? Závisí to na objemu pracovní zátěže ve správci front a na mísení provozu, například o tom, jak velká část je trvalá, v rámci synchronizačního bodu a jak velká část byla potvrzena před selháním. IBM testů failover a failback time of about a minute. To bylo na velmi lehce zatíženém správci front a skutečné časy se značně liší v závislosti na zatížení.

Ověření, že MSCS pracuje

Postupujte takto, abyste se ujistili, že máte spuštěný klastr MSCS.

Popisy úloh začínající řetězcem [“Vytvoření správce front pro použití se službou MSCS”](#) na stránce 388 předpokládají, že máte spuštěný klastr MSCS, v rámci kterého můžete vytvářet, migrovat a odstraňovat prostředky. Chcete-li se ujistit, že máte takový klastr:

1. Pomocí administrátora klastru MSCS vytvořte skupinu.
2. V rámci této skupiny vytvořte instanci generického prostředku aplikace a zadejte systémové hodiny (název cesty C:\winnt\system32\clock.exe a pracovní adresář produktu C:\).
3. Ujistěte se, že můžete prostředek převést online, že můžete přesunout skupinu, která ji obsahuje, do jiného uzlu, a že můžete prostředek převést do stavu offline.

Ruční spuštění

Pro správce front spravovaného službou MSCS **musíte** nastavit atribut spuštění na ruční. Tím je zajištěno, že podpora serveru IBM MQ MSCS může restartovat službu MQSeries bez okamžitého spuštění správce front.

Podpora produktu IBM MQ MSCS musí být schopna restartovat službu, aby mohla provádět monitorování a řízení, ale sama musí zůstat v řízení, které správci front jsou spuštěny a na kterých počítačích. Další informace viz [“Přesun správce front do úložiště MSCS”](#) na stránce 389.

MSCS a správce front

Aspekty týkající se správců front při použití MSCS.

Vytvoření odpovídajícího správce front v jiném uzlu

Chcete-li klastrování pracovat s produktem IBM MQ, potřebujete stejného správce front v uzlu B pro každý uzel na uzlu A. Avšak, nemusíte výslovně vytvářet druhou. Správce front můžete vytvořit nebo připravit na jednom uzlu, přesunout jej do jiného uzlu, jak je popsáno v tématu [“Přesun správce front do úložiště MSCS”](#) na stránce 389, a je na daném uzlu plně duplikován.

Výchozí správci front

V rámci ovládacího prvku MSCS nepoužívejte výchozího správce front. Správce front nemá vlastnost, která z něj činí výchozí hodnotu; produkt IBM MQ uchovává svůj vlastní samostatný záznam. Přesunete-li sadu správců front jako výchozí nastavení na jiný počítač v případě překonání selhání, nestane se výchozí hodnotou. Upravte všechny aplikace tak, aby odkazovaly na specifické správce front podle názvu.

Odstranění správce front

Jakmile má správce front přesunutý uzel, jeho podrobnosti existují v registru na obou počítačích. Chcete-li jej odstranit, proveďte to jako normální na jednom počítači a poté spusťte obslužný program popsáný v tématu [“IBM MQ programy obslužného programu pro podporu MSCS”](#) na stránce 400, abyste vyčistili registr na jiném počítači.

Podpora pro existující správce front

Existující správce front můžete umístit pod ovládací prvek MSCS za předpokladu, že můžete umístit soubory protokolu správce front a soubory fronty na disk, který se nachází na sdílené sběrnici SCSI mezi dvěma počítači (viz [Obrázek 73](#) na stránce 386). Při vytvoření prostředku MSCS je třeba správce front krátce převést do stavu offline.

Chcete-li vytvořit nového správce front, vytvořte jej nezávisle na serveru MSCS, otestujte jej a poté jej umístěte pod ovládací prvek MSCS. Viz:

- [“Vytvoření správce front pro použití se službou MSCS”](#) na stránce 388
- [“Přesun správce front do úložiště MSCS”](#) na stránce 389
- [“Vložení správce front do ovládacího prvku MSCS”](#) na stránce 390

Vykazování MSCS, které správci front mají spravovat

Vybíráte, kteří správci front jsou umístěni pod řízením MSCS, pomocí administrátora klastru MSCS, aby bylo možné vytvořit instanci prostředku pro každého takového správce front. Tento proces vám předkládá seznam prostředků, ze kterých chcete vybrat správce front, kterého chcete spravovat.

Soubory protokolu správce front

Přesunete-li správce front do úložiště MSCS, přesunete jeho protokol a datové soubory na sdílený disk (viz příklad [“Přesun správce front do úložiště MSCS” na stránce 389](#)).

Před přesunem je vhodné správce front řádně vypnout a provést úplné zálohování datových souborů a souborů protokolu.

Více správců front

Podpora MSCS produktu IBM MQ vám umožňuje spouštět více správců front v každém počítači a umísťovat jednotlivé správce front v rámci řízení MSCS.

Vždy použít službu MSCS pro správu klastrů

Nepokoušejte se provádět operace spuštění a zastavení přímo na libovolném správci front pod kontrolou MSCS pomocí řídicích příkazů nebo Průzkumníka IBM MQ. Místo toho použijte administrátora klastru MSCS k převedení správce front do režimu online nebo jej převedte do stavu offline.

Použití programu MSCS Cluster Administrator je částečně zamezené případným nejasnostem způsobenému hlášením MSCS, že je správce front offline, kdy jste jej spustili mimo kontrolu prostředí MSCS. Přesněji řečeno, zastavení správce front bez použití serveru MSCS bylo zjištěno serverem MSCS jako selhání, čímž se iniciuje překonání selhání na jiný uzel.

Práce v aktivním/aktivním režimu

Oba počítače v klastru MSCS mohou spouštět správce front v aktivním/aktivním režimu. Nemusíte mít plně nečinný počítač fungující jako záložní (ale pokud chcete, můžete, pokud chcete, v režimu Aktivní/Pasivní režim).

Plánujete-li používat ke spuštění pracovní zátěže oba stroje, poskytněte každému s dostatečnou kapacitou (procesor, paměť, sekundární paměť), aby se na uspokojivé úrovni výkonu spouštěla celková pracovní zátěž klastru.

Poznámka: Používáte-li službu MSCS spolu se serverem Microsoft Transaction Server (COM +), **nelze** použít režim aktivní/aktivní. Je tomu tak proto, že pro použití produktu IBM MQ s MSCS a COM +:

- Komponenty aplikace, které používají podporu COM + IBM MQ, musí být spuštěny na stejném počítači jako koordinátor distribuovaných transakcí (DTC), část COM +.
- Správce front musí být také spuštěn na stejném počítači.
- DTC musí být konfigurována jako prostředek MSCS, a proto může být spuštěna na jednom z počítačů v klastru kdykoli.

Příkaz PostOnlinea příkaz PreOffline

Tyto příkazy použijte k integraci podpory MSCS produktu IBM MQ s jinými systémy. Můžete je použít k vydání příkazu IBM MQ, některá omezení vzh.

Určete tyto příkazy v parametrech pro prostředek typu IBM MQ MSCS. Můžete je použít k integraci podpory MSCS produktu IBM MQ s jinými systémy nebo procedurami. Můžete například zadat název programu, který odesílá poštovní zprávu, aktivuje pager nebo vygeneruje nějakou jinou formu výstrahy, která má být zachycována jiným systémem monitorování.

Příkaz PostOnlineje vyvolán, když se prostředek změní z režimu offline do režimu online; příkaz PreOfflineje vyvolán pro změnu z režimu online do režimu offline. Při vyvolání jsou tyto příkazy spuštěny standardně ze systémového adresáře Windows. Protože IBM MQ používá 32bitový proces monitorování prostředků, na 64bitových systémech Windows se jedná o adresář `\Windows\SysWOW64` spíše než na adresář `\Windows\system32`. Další informace naleznete v dokumentaci produktu Microsoft

o přesměrování souboru v prostředí Windows x64 . Oba příkazy běží pod uživatelským účtem, který se používá ke spuštění služby MSCS, a jsou vyvoláni asynchronně; IBM MQ podpora MSCS nečeká na dokončení zpracování, než bude pokračovat. Tím vyloučíte jakékoli riziko, že by mohly blokovat nebo zpožďovat další operace klastru.

Tyto příkazy můžete také použít k vydání příkazů IBM MQ , například k restartování žadatelských kanálů. Příkazy se však spouštějí v daném okamžiku, kdy se změní stav správce front, takže nejsou určeny k provádění dlouhodobě spuštěných funkcí a nesmí vytvářet předpoklady o aktuálním stavu správce front; je zcela možné, že ihned po uvedení správce front do stavu online administrátor vydal příkaz offline.

Chcete-li spouštět programy, které závisí na stavu správce front, zvažte vytvoření instancí typu prostředku MSCS Generic Application , jejich umístění do stejné skupiny MSCS jako prostředek správce front a jejich zpřístupnění v závislosti na prostředku správce front.

Použití preferovaných uzlů

To může být užitečné, když používáte Aktivní/Aktivní režim ke konfiguraci *upřednostňovaného uzlu* pro každého správce front. Obecně je však lepší nenastavit upřednostňovaný uzel, ale spoléhat se na ruční odvolání při selhání.

Na rozdíl od jiných relativně nestavových prostředků může správce front provést převedení z jednoho uzlu na druhý uzel (nebo zpět). Chcete-li se vyhnout zbytečným výpadkům, otestujte obnovený uzel předtím, než k němu dojde k selhání správce front. Toto znemožňuje použití nastavení odvolání při selhání *immediate* . Můžete nakonfigurovat návrat po selhání, aby se vyskytl mezi určitými časy dne.

Nejbezpečnější cestou je pravděpodobně přesunout správce front zpět ručně do požadovaného uzlu, když jste si jisti, že uzel je zcela obnoven. Toto vylučuje použití volby *preferred node* .

Pokud se v protokolu událostí aplikace vyskytnou chyby COM +

Při instalaci produktu IBM MQ v nově nainstalovaném klastru MSCS může být nalezena chyba se zdrojem COM + a ID události 4691, hlášeným v protokolu událostí aplikace.

To znamená, že se pokoušíte spustit produkt IBM MQ v prostředí serveru Microsoft Cluster Server (MSCS), když se Microsoft Distributed Transaction Coordinator (MSDTC) nekonfiguroval tak, aby se spouštěl v takovém prostředí. Informace o konfiguraci produktu MSDTC v klastrovaném prostředí najdete v dokumentaci produktu Microsoft .

IBM MQ programy obslužného programu pro podporu MSCS

Seznam podpory IBM MQ pro obslužné programy MSCS, které můžete spustit na příkazovém řádku.

Podpora produktu IBM MQ pro službu MSCS zahrnuje následující obslužné programy:

Registrace/zrušení registrace typu prostředku

`haregtyp.exe`

Po *zrušení registrace* typu prostředku IBM MQ MSCS již nebudete moci vytvářet žádné prostředky tohoto typu. MSCS vám nezruší registraci typu prostředku, pokud stále máte instance tohoto typu v klastru:

1. Pomocí správce klastrů MSCS zastavte všechny správce front, kteří jsou spuštěni v rámci řízení MSCS, tak, že je budete v režimu offline, jak je popsáno v tématu [“Převedení správce front do režimu offline z prostředí MSCS”](#) na stránce 397.
2. Pomocí administrátora klastru MSCS odstraňte instance prostředků.
3. Na příkazovém řádku zrušte registraci tohoto typu prostředku zadáním následujícího příkazu:

```
haregtyp /u
```

Chcete-li *registrovat* typ (nebo jej znovu zaregistrovat později), zadejte na příkazový řádek následující příkaz:

```
haregtyp /r
```


Po úspěšné registraci knihoven MSCS je třeba restartovat systém, pokud jste tak neučinili od instalace produktu IBM MQ.

Přesunout správce front do úložiště MSCS

hamvmqm.exe

Viz [“Přesun správce front do úložiště MSCS”](#) na stránce 389.

Odstranit správce front z uzlu

hadltmqm.exe

Předpokládejme případ, kdy jste ve svém klastru měli správce front, byl přesunut z jednoho uzlu do jiného uzlu a nyní jej chcete zničit. Použijte program Průzkumník IBM MQ k jeho odstranění na uzlu, kde aktuálně je. Položky registru pro ni stále existují na jiném počítači. Chcete-li je odstranit, zadejte na příkazový řádek v tomto počítači následující příkaz:

```
hadltmqm /m qmname
```

kde qmname je název správce front, který má být odebrán.

Podrobnosti o nastavení kontroly a uložení

amqmsysn.exe

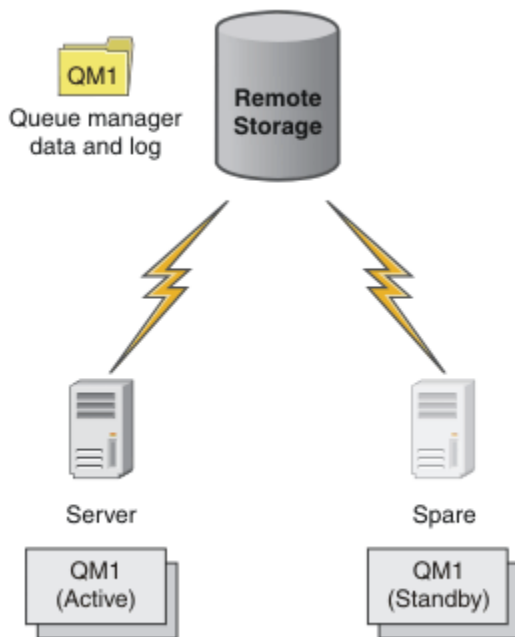
Tento obslužný program zobrazí dialogové okno s úplnými podrobnostmi o nastavení podpory MSCS produktu IBM MQ, jako je například výzva k volání podpory produktu IBM. K dispozici je volba pro uložení podrobností do souboru.

Správci front s více instancemi

Správci front s více instancemi jsou instance stejného správce front konfigurovaného na různých serverech. Jedna instance správce front je definována jako aktivní instance a jiná instance je definována jako instance v pohotovostním režimu. Dojde-li k selhání aktivní instance, správce front s více instancemi se automaticky restartuje na záložním serveru.

Příklad konfigurace správce front s více instancemi

Obrázek 74 na stránce 402 uvádí příklad konfigurace s více instancemi pro správce front QM1. Produkt IBM MQ je nainstalován na dvou serverech, z nichž jeden je volný. Byl vytvořen jeden správce front QM1. Jedna instance QM1 je aktivní a je spuštěna na jednom serveru. Druhá instance serveru QM1 je spuštěna v pohotovostním režimu na druhém serveru, neprovádí žádné aktivní zpracování, ale je připravena převzít z aktivní instance QM1, pokud se aktivní instance nezdaří.



Obrázek 74. Správce front s více instancemi

Zamýšlíte-li používat správce front jako správce front s více instancemi, vytvořte jednoho správce front na jednom ze serverů pomocí příkazu **crtmqm**, který umístí data správce front a protokoly do sdílené síťové paměti. Na jiném serveru, než znovu vytvořit správce front, použijte příkaz **addmqinf** k vytvoření odkazu na data správce front a protokoly v síťovém úložišti.

Nyní můžete správce front spustit z jednoho ze serverů. Každý ze serverů odkazuje na stejná data a protokoly správce front; existuje pouze jeden správce front a v daném okamžiku je aktivní pouze na jednom serveru.

Správce front může být spuštěn buď jako správce front s jednou instancí, nebo jako správce front s více instancemi. V obou případech je spuštěna pouze jedna instance správce front, zpracování požadavků. Rozdíl je v tom, že při spuštění jako správce front s více instancemi se server, na kterém není spuštěna aktivní instance správce front, spustí jako instance v pohotovostním režimu, je připraven převzít z aktivní instance automaticky, pokud selže aktivní server.

Jediný ovládací prvek, který je nad kterými instancí se stane aktivní, je pořadí, ve kterém spustíte správce front na obou serverech. První instance, která získá zámky pro čtení a zápis do dat správce front, se stane aktivní instancí.

Aktivní instanci můžete odložit na jiný server, jakmile se spustí, tím, že zastavíte aktivní instanci pomocí volby přepnutí na přenos do pohotovostního režimu.

Aktivní instance QM1 má výlučný přístup k datům správce sdílených front a ke složkám protokolů, je-li spuštěn. Rezervní instance QM1 zjišťuje, kdy došlo k selhání aktivní instance, a stane se aktivní instancí. Přebírá data a protokoly QM1 ve stavu, kdy byly ponechány aktivní instancí, a přijímá nová připojení od klientů a kanálů.

Aktivní instance může selhat z různých příčin, které vedou k převzetí stavu pohotovosti:

- Selhání serveru hostujícího aktivní instanci správce front.
- Selhání konektivity mezi serverem, který je hostitelem aktivní instance správce front, a systému souborů.
- Neschopnost reagovat na procesy správce front detekovaná produktem IBM MQ, která poté ukončí práci správce front.

Informace o konfiguraci správce front můžete přidat na více serverů a vybrat libovolné dva servery, které se mají spustit jako dvojice aktivní/záložní. Existuje zde limit celkového počtu dvou instancí. Nemůžete mít dvě instance v pohotovostním režimu a jednu aktivní instanci.

Další komponenty potřebné k sestavení řešení vysoké dostupnosti

Správce front pro více instancí je jednou částí řešení vysoké dostupnosti. Chcete-li vytvořit užitečné řešení vysoké dostupnosti, potřebujete další komponenty.

- Připojení klienta a kanálu pro přenos IBM MQ připojení k počítači, který přebírá spuštění aktivní instance správce front.
- Vysoce výkonný sdílený síťový systém souborů (NFS), který spravuje zámky správně a poskytuje ochranu proti selhání média a souborového serveru.

Důležité: Před prováděním údržby na jednotce NFS je třeba zastavit všechny instance správce front s více instancemi, které jsou spuštěny ve vašem prostředí. V případě selhání systému NFS se ujistěte, že máte zálohy konfigurace správce front, které se mají obnovit.

- Spolehlivé sítě a zdroje napájení za účelem odstranění jednotných bodů selhání v základní infrastruktuře.
- Aplikace tolerují překonání selhání. Zejména je třeba věnovat pozornost chování transakčních aplikací a aplikací, které procházejí fronty produktu IBM MQ .
- Monitorování a správa aktivních instancí a instancí v pohotovostním režimu za účelem zajištění jejich spuštění a restartování aktivních instancí, které selhaly. Ačkoli se správce front s více instancemi restartuje automaticky, musíte se ujistit, že jsou vaše instance v pohotovostním režimu spuštěny, připraveny převzít převzetí a že instance se selháním jsou znovu uvedeny do stavu online jako nové instance v pohotovostním režimu.

IBM MQ MQI clients a kanály se znovu automaticky připojí ke správci front v pohotovostním režimu, jakmile se stane aktivním. Další informace o opětovném připojení a další komponenty v řešení vysoké dostupnosti najdete v souvisejících tématech. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

podporované platformy

Správce front s více instancemi můžete vytvořit na libovolné platformě jiné než z/OS podporované produktem IBM MQ z produktu IBM WebSphere MQ 7.0.1.

Automatické opětovné připojení klienta je podporováno pro klienty MQI od produktu IBM WebSphere MQ 7.0.1 .

Vytvoření správce front s více instancemi

Vytvoření správce front s více instancemi, vytvoření správce front na jednom serveru a konfigurace produktu IBM MQ na jiném serveru. Správci front s více instancemi sdílejí data a protokoly správce front.

Většina úsilí zapojování do vytváření správce front s více instancemi je úlohou nastavení dat správce sdílené fronty a souborů protokolu. Musíte vytvořit sdílené adresáře v síťovém úložišti a zpřístupnit adresáře pro jiné servery pomocí sdílených síťových sdílených složek. Tyto úlohy je třeba provést někým, kdo má administrativní oprávnění, jako je *root* na systémech SYSTÉM UNIX a Linux . Kroky jsou následující:

1. Vytvořte sdílené prostředky pro data a soubory protokolu.
2. Vytvořte správce front na jednom serveru.
3. Spuštěním příkazu **dspmqlnf** na prvním serveru shromáždíte konfigurační data správce front a zkopírujete je do schránky.
4. Spusťte příkaz **addmqinf** s zkopírovanými daty za účelem vytvoření konfigurace správce front na druhém serveru.

Nespustíte příkaz **crtmqm** k opětovnému vytvoření správce front na druhém serveru.

Řízení přístupu k souboru

Je třeba dbát na to, aby uživatel a skupina *mqm* na všech ostatních serverech měly oprávnění pro přístup ke sdílením.

V systému SYSTÉM UNIX a Linux musíte ve všech systémech učinit uid a gid produktu mqm stejné. Možná budete muset upravit /etc/passwd na každém systému, abyste nastavili obecné uid a gid pro mqm, a pak znovu zavedte systém.

V systému Microsoft Windows musí mít ID uživatele, který spouští procesy správce front, úplné oprávnění pro řízení k adresářům obsahujícím data správce front a soubory protokolu. Oprávnění můžete nakonfigurovat dvěma způsoby:


1. Vytvořte správce front s globální skupinou jako alternativního činitele zabezpečení. Autorizujte globální skupinu, aby měla úplný přístup pro řízení k adresářům obsahujícím data správce front a soubory protokolu, viz [“Zabezpečte data správce sdílených front a soubory protokolu a soubory v systému Windows”](#) na stránce 431. Vytvořte ID uživatele, pod kterým je spuštěn správce front, člena globální skupiny. Lokální uživatele nelze vytvořit jako člena globální skupiny, takže procesy správce front musí být spuštěny pod ID uživatele domény. ID uživatele domény musí být členem lokální skupiny mqm. Úloha [“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény”](#) na stránce 406 demonstruje, jak nastavit správce front s více instancemi pomocí souborů zabezpečených tímto způsobem.
2. Vytvořte správce front v řadiči domény tak, aby lokální skupina mqm měla rozsah domény, "lokální doména". Zabezpečte sdílení souboru s lokálním serverem mqm a spusťte procesy správce front ve všech instancích správce front v rámci stejné lokální skupiny produktu mqm. Úloha [“Vytvoření správce front s více instancemi na řadičích domény”](#) na stránce 421 demonstruje, jak nastavit správce front s více instancemi pomocí souborů zabezpečených tímto způsobem.


Informace o konfiguraci


Nakonfigurujte tolik instancí správce front, kolik potřebujete, úpravou informací o konfiguraci správce front produktu IBM MQ na každém serveru. Každý server musí mít nainstalovanou stejnou verzi produktu IBM MQ na kompatibilní úrovni oprav. Příkazy, **dspmqlinf** a **addmqinf** vám pomáhají konfigurovat další instance správce front. Alternativně můžete soubory mqs.ini a qm.ini upravit přímo. Témata, [“Vytvoření správce front s více instancemi v systému Linux”](#) na stránce 443, [“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény”](#) na stránce 406a [“Vytvoření správce front s více instancemi na řadičích domény”](#) na stránce 421 představují příklady konfigurace správce front s více instancemi.

V systémech Windows, SYSTÉM UNIX a Linux můžete sdílet jeden soubor mqs.ini tak, že jej umístíte na sdílenou síťovou stránku a nastavíte proměnnou prostředí **AMQ_MQS_INI_LOCATION** tak, aby ukazovala na jeho hodnotu.

Omezení

1. Konfigurovat více instancí stejného správce front pouze na serverech se stejným operačním systémem, architekturou a endiannem. Oba stroje musí být například buď 32bitové, nebo 64bitové.
2. Všechny instalace produktu IBM MQ musí být na úrovni verze 7.0.1 nebo vyšší.
3. Typicky jsou aktivní a záložní instalace udržovány na stejné úrovni údržby. Chcete-li zkontrolovat, zda je třeba provést upgrade všech instalací, prostudujte si pokyny k údržbě pro každý přechod na vyšší verzi. Všimněte si, že úroveň údržby aktivních a pasivních správců front musí být identické.
4. Sdílejte data správce front a protokoly pouze mezi správci front, kteří jsou konfigurováni se stejným uživatelem produktu IBM MQ, skupinou a mechanismem řízení přístupu.  Například sdílení sítě nastavené na serveru Linux může obsahovat samostatná data správce front a protokoly pro správce front produktu SYSTÉM UNIX a Linux, ale nemůže obsahovat data správce front, která byla použita produktem IBM i.

 Můžete vytvořit více sdílených prostředků ve stejném síťovém úložišti pro produkt IBM i a další Systémy SYSTÉM UNIX, pokud se sdílení liší. Odlišné vlastníky můžete dát různým vlastníkům. Omezení je důsledkem různých názvů používaných pro uživatele a skupiny produktu IBM MQ mezi produkty UNIX a IBM i. Skutečnost, že uživatel a skupina mohou mít stejné uid a gid, nezklidňuje omezení.

5. V systémech SYSTÉM UNIX a Linux nakonfigurujte sdílený systém souborů v síťovém úložišti pomocí volby `hard`, přerušitelný, místo připojení `soft`. Pevné přerušitelné připojení vynutí, aby správce front uvázl, dokud nebude přerušeno systémem voláním. Měkká připojení nezaručují konzistenci dat po selhání serveru.
6. Sdílený protokol a datové adresáře nemohou být uloženy v systému souborů FAT nebo v systému souborů NFSv3. Pro správce front s více instancemi v systému Windows musí být k síťovému úložišti přistupovat prostřednictvím protokolu CIFS (Common Internet File System) používaného sítěmi Windows.
7.  Produkt z/OS nepodporuje správce front s více instancemi. Použít skupiny sdílení front. Znovu připojitelné klienty pracují se správci front produktu z/OS.

Windows domén a správců front s více instancemi

Správce front s více instancemi v produktu Windows vyžaduje, aby byla sdílena data a protokoly. Sdílení musí být přístupné pro všechny instance správce front spuštěných na různých serverech nebo pracovních stanicích. Konfigurujte správce front a sdílejte jej jako součást domény produktu Windows. Správce front může být spuštěn na pracovní stanici nebo na serveru domény nebo na řadiči domény.

Před konfigurací správce front s více instancemi si přečtěte téma [“Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows”](#) na stránce 434 a [“Zabezpečte data správce sdílených front a soubory protokolu a soubory v systému Windows”](#) na stránce 431 a zkontrolujte, jak řídit přístup k datům správce front a protokolových souborů. Témata jsou vzdělávací; chcete-li přejít přímo k nastavení sdílených adresářů pro správce front s více instancemi v doméně Windows, viz [“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény”](#) na stránce 406.

Spustit správce front s více instancemi na pracovních stanicích nebo na serverech domény

V produktu Verze 7.1 jsou správci front s více instancemi spouštěny na pracovní stanici nebo na serveru, který je členem domény. Před Verze 7.1 se správci front pro více instancí spouštěli pouze na řadičích domény, viz [“Spustit správce front s více instancemi na řadičích domény”](#) na stránce 406. Chcete-li spustit správce front s více instancemi v produktu Windows, je třeba mít k dispozici řadič domény, souborový server a dvě pracovní stanice nebo servery provozující stejného správce front připojeného ke stejné doméně.

Změna, která umožňuje spustit správce front s více instancemi na libovolném serveru nebo pracovní stanici v doméně, je to, že můžete nyní vytvořit správce front s další skupinou zabezpečení. Další skupina zabezpečení je předána v příkazu `crtmqm`, v parametru `-a`. Zabezpečte adresáře, které obsahují data správce front, a protokoly se skupinou. ID uživatele, který spouští procesy správce front, musí být členem této skupiny. Když správce front přistupuje k adresářům, produkt Windows zkontroluje oprávnění, která má ID uživatele pro přístup k adresářům. Uvede-li skupina i rozsah domény ID uživatele, bude mít ID uživatele, který spouští procesy správce front, pověření z globální skupiny. Je-li správce front spuštěn na jiném serveru, může mít ID uživatele, který spouští procesy správce front, stejná pověření. ID uživatele nemusí být stejné. Musí být členem alternativní skupiny zabezpečení, stejně jako člen lokální skupiny `mqm`.

Úloha vytvoření správce front s více instancemi je stejná jako v produktu Verze 7.0.1 s jednou změnou. Do parametrů příkazu `crtmqm` je třeba přidat název další skupiny zabezpečení. Úloha je popsána v tématu [“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény”](#) na stránce 406.

Pro konfiguraci domény a pro servery a pracovní stanice domény je třeba provést více kroků. Je třeba pochopit, jak produkt Windows autorizuje přístup správce front k jeho datům a adresářům protokolů. Pokud si nejste jisti, jak jsou procesy správce front autorizovány pro přístup k protokolové a datové soubory, přečtěte si téma [“Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows”](#) na stránce 434. Toto téma obsahuje dvě úlohy, které vám pomohou porozumět krokům, které je třeba provést. Úlohy jsou [“Čtení a zápis dat a souborů protokolu registrovaných lokální skupinou produktu mqm”](#) na stránce 436 a [“Čtení a zápis dat a souborů protokolu, které jsou autorizovány alternativní lokální skupinou zabezpečení”](#) na stránce 439. Další téma, [“Zabezpečte data](#)

správce sdílených front a soubory protokolu a soubory v systému Windows” na stránce 431, vysvětluje, jak zabezpečit sdílené adresáře obsahující data správce front a soubory protokolu s alternativní skupinou zabezpečení. Toto téma obsahuje čtyři úlohy pro nastavení domény produktu Windows , vytvoření sdílení souboru, instalaci produktu IBM MQ for Windowsa konfigurování správce front pro použití sdílení. Úlohy jsou následující:

1. [“Vytvoření Active Directory a domény DNS pro IBM MQ”](#) na stránce 409.
2. [“Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows”](#) na stránce 413.
3. [“Vytvoření sdíleného adresáře pro data správce front a soubory protokolu”](#) na stránce 415.
4. [“Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení”](#) na stránce 418.

Potom můžete provést úlohu [“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény”](#) na stránce 406 pomocí domény. Tyto úlohy slouží k prozkoumání nastavení správce front pro více instancí před přenosem vašich znalostí do produkční domény.

Spustit správce front s více instancemi na řadičích domény

Ve správci Verze 7.0.1 běžely správci front více instancí pouze na řadičích domény. Data správce front by mohla být zabezpečena pomocí skupiny domén `mqm` . Jak se vysvětluje téma [“Zabezpečte data správce sdílených front a soubory protokolu a soubory v systému Windows”](#) na stránce 431 , nemůžete sdílet adresáře zabezpečené s lokální skupinou `mqm` na pracovních stanicích nebo serverech. Avšak na řadičích domény všechny skupiny a řídicí služby mají rozsah domény. Pokud instalujete produkt IBM MQ for Windows na řadič domény, data správce front a soubory protokolu jsou zabezpečeny skupinou `mqm` domény, kterou lze sdílet. Postupujte podle kroků uvedených v úloze [“Vytvoření správce front s více instancemi na řadičích domény”](#) na stránce 421 a nakonfigurujte správce front s více instancemi na řadičích domény.

Související informace

[Správa autorizace a řízení přístupu](#)

[Jak používat uzly klastru serveru Windows jako řadiče domény](#)

Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény

Příklad ukazuje, jak nastavit správce front s více instancemi na systému Windows na pracovní stanici nebo na serveru, který je součástí domény Windows . Server nemusí být řadič domény. Nastavení demonstruje zahrnuté koncepce, spíše než aby bylo produkční měřítko. Tento příklad je založen na serveru Windows Server 2008. Tyto kroky se mohou lišit od dalších verzí serveru Windows .

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun

Řadič domény produktu Windows Server 2008. Je vlastníkem domény `wmq.example.com` , která obsahuje `sun` , `mars` a `venus` . Pro účely ilustrace se používá také jako souborový server.

mars

Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem `QMGR` .

venus

Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem `QMGR` .

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

V systému Windows není nutné ověřovat systém souborů, do kterého chcete ukládat data správce front a soubory žurnálu. Procedura kontroly, Ověření chování sdíleného systému souborů, je použitelná pro SYSTÉM UNIX a Linux. V systému Windows jsou kontroly vždy úspěšné.

Postupujte podle kroků uvedených v následujících úlohách. Úlohy vytvoří řadič domény a doménu, nainstalujte produkt IBM MQ for Windows na jeden server a vytvořte sdílení souboru pro data a soubory protokolu. Pokud konfiguruje existující řadič domény, můžete zjistit, že je užitečné vyzkoušet si kroky na novém serveru Windows Server 2008. Kroky je možné upravit podle své domény.

1. “Vytvoření Active Directory a domény DNS pro IBM MQ” na stránce 409.
2. “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 413.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu” na stránce 415.
4. “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 418.

Informace o této úloze

Tato úloha je jednou z posloupností úloh pro konfiguraci řadiče domény a dvou serverů v doméně za účelem spuštění instancí správce front. V této úloze nakonfigurujete druhý server, produkt *venus*, aby spustil jinou instanci správce front *QMGR*. Postupujte podle kroků uvedených v této úloze a vytvořte druhou instanci správce front, *QMGR* a otestujte, zda pracuje.

Tato úloha je oddělena od čtyř úloh v předchozí sekci. Obsahuje kroky, které převádějí jednoho správce front instance na správce front s více instancemi. Všechny ostatní kroky jsou společné pro jednotlivé správce front nebo správce front s více instancemi.

Postup

1. Nakonfigurujte druhý server ke spuštění produktu IBM MQ for Windows.
 - a) Chcete-li vytvořit druhý server domény, proveďte kroky v úloze “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 413. V této posloupnosti úloh se druhý server nazývá *venus*.

Tip: Vytvořte druhou instalaci s použitím stejných výchozích nastavení instalace pro produkt IBM MQ na každém ze dvou serverů. Pokud se výchozí hodnoty liší, možná budete muset upravit proměnné `Předpona` a `InstallationName` ve stanici *QMGR QueueManager* v konfiguračním souboru IBM MQ `mqs.ini`. Proměnné odkazují na cesty, které se mohou lišit pro každou instalaci a správce front na každém serveru. Pokud cesty zůstávají stejné na každém serveru, je jednodušší konfigurovat správce front s více instancemi.
2. Vytvořte druhou instanci produktu *QMGR* v systému *venus*.
 - a) Pokud *QMGR* v systému *mars* neexistuje, proveďte úlohu “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 418a vytvořte ji.
 - b) Zkontrolujte hodnoty parametrů `Předpona` a `InstallationName`, které jsou správné pro produkt *venus*.

V systému *mars* spusťte příkaz **dspmqlinf**:

```
dspmqlinf QMGR
```

Odezva systému:

```
QueueManager:  
Name=QMGR  
Directory=QMGR
```

```
Prefix=C:\ProgramData\IBM\MQ
DataPath=\\sun\wmq\data\QMGR
InstallationName=Installation1
```

- c) Okopírujte strojově čitelnou formu stanzy **QueueManager** do schránky.

V systému *mars* spusťte příkaz **dspmqlnf** znovu s parametrem `-o command` .

```
dspmqlnf -o command QMGR
```

Odezva systému:

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

- d) V systému *venus* spusťte příkaz **addmqinf** ze schránky a vytvořte instanci správce front v systému *venus* .

V případě potřeby upravte příkaz tak, aby vyhovoval rozdílům v parametrech Předpona nebo `InstallationName` .

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

IBM MQ configuration information added.

3. Spusťte správce front *QMGR* v systému *venus* a povolte instance v pohotovostním režimu.

- a) Kontrola *QMGR* na *mars* je zastavena.

V systému *mars* spusťte příkaz **dspmql** :

```
dspmql -m QMGR
```

Odezva systému závisí na tom, jak byl správce front zastaven; například:

```
C:\Users\Administrator>dspmql -m QMGR
QMNAME(QMGR) STATUS(Ended immediately)
```

- b) V systému *venus* spusťte příkaz **strmqm** ke spuštění příkazu *QMGR* , který povoluje standbys:

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

Výsledky

Chcete-li otestovat přepínače správce front s více instancemi, proveďte následující kroky:

1. V systému *mars* spusťte příkaz **strmqm**, který spustí příkaz *QMGR* povolující standby:

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.  
The queue manager is associated with installation 'Installation1'.  
A standby instance of queue manager 'QMGR' has been started.  
The active instance is running elsewhere.
```

2. V systému *venus* spusťte příkaz **endmqm**:

```
endmqm -r -s -i QMGR
```

Odezva systému na *venus*:

```
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ended, permitting switchover to  
a standby instance.
```

A v systému *mars*:

```
dspmqr  
QMNAME(QMGR) STATUS(Running as standby)  
C:\Users\wmquser2>dspmqr  
QMNAME(QMGR) STATUS(Running as standby)  
C:\Users\wmquser2>dspmqr  
QMNAME(QMGR) STATUS(Running)
```

Jak pokračovat dále

Chcete-li ověřit správce front s více instancemi pomocí ukázkových programů, přečtěte si téma [“Ověřte správce front s více instancemi v systému Windows”](#) na stránce 429.

Vytvoření Active Directory a domény DNS pro IBM MQ

Tato úloha vytvoří doménu *wmq.example.com* na řadiči domény Windows 2008 s názvem *sun*. Nakonfiguruje globální skupinu *Domain mqm* v doméně, se správnými právy a s jedním uživatelem.

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun

Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com*, která obsahuje *Sun*, *mars* a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars

Server Windows Server 2008 použitý jako první server IBM MQ. Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus

Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR* .

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Kroky úlohy jsou konzistentní s produktem Windows Server 2008, který je nainstalován, ale není nakonfigurován s žádnou rolí. Pokud konfiguruje existující řadič domény, můžete zjistit, že je užitečné vyzkoušet si kroky na novém serveru Windows Server 2008. Kroky je možné upravit podle své domény.

Informace o této úloze

V této úloze vytvoříte Active Directory a doménu DNS na novém řadiči domény. Poté ji nakonfiguruje tak, aby byl připraven k instalaci produktu IBM MQ na jiných serverech a pracovních stanicích, které se připojí k doméně. Pokud nejste obeznámeni s instalací a konfigurací adresáře Active Directory pro vytvoření domény produktu Windows , postupujte podle této úlohy. Chcete-li vytvořit konfiguraci správce front s více instancemi, je třeba vytvořit doménu produktu Windows . Úloha není určena k tomu, aby vás nejlépe vedla ke konfiguraci domény produktu Windows . Chcete-li implementovat správce front s více instancemi v produkčním prostředí, musíte se seznámit s dokumentací produktu Windows .

Během úlohy proveďte následující kroky:

1. Nainstalujte Active Directory.
2. Přidejte doménu.
3. Přidejte doménu do DNS.
4. Vytvořte globální skupinu `Domain mqm` a udělte mu správná práva.
5. Přidejte uživatele a vytvořte jej jako člena globální skupiny `Domain mqm`.

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolů uložených v adresáři dle vaší volby. Jsou připojeny k úloze, [“Windows domén a správců front s více instancemi”](#) na stránce 405.

Pro účely úlohy je název hostitele řadiče domény *sun* a tyto dva servery IBM MQ se nazývají *mars* a *venus* . Doména se nazývá *wmq.example.com* . Všechny kurzívy v úloze můžete nahradit názvy dle vlastního výběru.

Postup

1. Přihlaste se k řadiči domény *sun* jako administrátor lokálního systému nebo administrátor produktu `Workgroup` .
Je-li server již konfigurován jako řadič domény, musíte se přihlásit jako administrátor domény.
2. Spusťte průvodce Active Directory Domain Services.
 - a) Klepněte na nabídku **Start > Spustit ...** Zadejte `dcprmo` a klepněte na **OK**.
Nejsou-li binární soubory Active Directory již nainstalovány, produkt Windows nainstaluje soubory automaticky.
3. V prvním okně průvodce ponechte zaškrtačací políčko **Použít rozšířenou instalaci režimu** prázdné.
Klepněte na tlačítko **Další > Další** a klepněte na volbu **Vytvořit novou doménu v novém lese > Další**.
4. Zadejte *wmq.example.com* do pole **FQDN kořenové domény lesa** . Klepněte na tlačítko **Další**.
5. V okně Nastavit funkční úroveň doménové struktury vyberte volbu **Windows Server 2003** nebo novější ze seznamu **Funkční úrovně doménové struktury > Další**.
Nejstarší úroveň serveru Windows , která je podporována produktem IBM MQ , je Windows Server 2003.

6. Volitelné: V okně Nastavit funkční úroveň domény vyberte volbu **Windows Server 2003** nebo novější ze seznamu **Funkční úrovně domény > Další**.

Tento krok je nezbytný pouze v případě, že nastavíte funkční úroveň doménové struktury na **Windows Server 2003**.

7. Otevře se okno Další volby řadiče domény s volbou **Server DNS** jako přidavnou volbou. Klepněte na tlačítko **Další a Ano**, chcete-li vymazat okno s varováním.

Tip: Je-li již server DNS nainstalován, tato volba se vám nepředkládá. Pokud chcete tuto úlohu sledovat přesně, odeberte všechny role z tohoto řadiče domény a začněte znovu.

8. Ponechejte adresáře Database, Log Files a SYSVOL nezměněných; klepněte na tlačítko **Další**.
9. Do polí **Heslo a Potvrdit heslo** zadejte heslo do pole Heslo administrátora režimu obnovy adresářových služeb. Klepněte na tlačítko **Další > Další**. V závěrečném okně průvodce vyberte volbu **Znovu spustit po dokončení**.
10. Když se řadič domény restartuje, přihlaste se jako *wmq\Administrator*.

Správce serveru se spustí automaticky.

11. Otevřete složku *wmq.example.com\Users*.

- a) Otevřete produkt **Server Manager > Role > Active Directory Domain Services > wmq.example.com > Users**.

12. Klepněte pravým tlačítkem myši na nabídku **Uživatelé > Nová > Skupina**.

- a) Do pole **Název skupiny** zadejte název skupiny.

Poznámka: Upřednostňovaný název skupiny je *Domain mqm*. Zadejte jej přesně tak, jak je uveden.

- Nazváním skupiny *Domain mqm* se upraví chování "Průvodce přípravou produktu IBM MQ" na pracovní stanici nebo serveru domény. Způsobí to, že "Průvodce přípravou produktu IBM MQ" automaticky přidá skupinu *Domain mqm* do lokální skupiny *mqm* v každé nové instalaci produktu IBM MQ v dané doméně.
- Pracovní stanice nebo servery můžete instalovat i v doméně bez globální skupiny *Domain mqm*. Pokud tak učiníte, musíte definovat skupinu se stejnými vlastnostmi, jaké má skupina *Domain mqm*. Tuto skupinu nebo uživatele, kteří jsou jejími členy, musíte určit jako členy lokální skupiny *mqm*, kdekoli je produkt IBM MQ v nějaké doméně nainstalován. Uživatele domény můžete zahrnout do více skupin. Vytvořte několik skupin domén, kde každá skupina odpovídá sadě instalací, kterou chcete spravovat samostatně. Uživatele domén rozdělte podle instalací, které spravují, do různých skupin domén. Přidejte každou skupinu domén nebo skupiny do lokální skupiny produktu *mqm* pro různé instalace produktu IBM MQ. Pouze uživatelé domény ve skupinách domén, které jsou členy specifické lokální skupiny *mqm*, mohou vytvářet, spravovat a spouštět správce front pro tuto instalaci.
- Uživatel domény, kterého navrhujete při instalaci produktu IBM MQ na pracovní stanici nebo server v doméně, musí být členem skupiny *Domain mqm* nebo alternativní skupiny, kterou jste definovali se stejnými vlastnostmi jako skupina *Domain mqm*.

- b) **Rozsah skupiny** ponechte **Globální**, případně jej můžete změnit na **Univerzální**. **Typ skupiny** ponechte jako **Zabezpečení**. Klepněte na tlačítko **OK**.

13. Přidejte práva, **Povolit Čist členství ve skupině** a **Povolit Čist groupMembershipSAM**, která se bude používat pro globální skupinu *Domain mqm*.

- a) V řádce s akcemi správce serveru klepněte na volbu **Pohled > Rozšířené vlastnosti**.

- b) Ve stromu navigace správce serveru klepněte na volbu **Uživatelé**.

- c) V okně *Users* klepněte pravým tlačítkem myši na položku **Domain mqm > Vlastnosti**.

- d) Klepněte na volbu **Zabezpečení > Rozšířené > Přidat ...**. Zadejte *Domain mqm* a klepněte na **Zkontrolovat jména > OK**.

Pole **Název** je předem vyplněno řetězcem *Domain mqm (domain name\Domain mqm)*.

- e) Klepněte na příkaz **Vlastnosti**. V seznamu **Použit na** vyberte položku **Podřízené objekty uživatele**.

- f) V seznamu **Oprávnění** vyberte zaškrťovací políčka **Čist členství ve skupině** a **Čist groupMembershipSAM Povolit** . Klepněte na tlačítko **OK > Použít > OK > OK** .

14. Přidejte dva nebo více uživatelů do globální skupiny Domain mqm .

Jeden uživatel, *wmquser1* v tomto příkladu, spouští službu IBM MQ a druhý uživatel, *wmquser2* , se používá interaktivně.

Pro vytvoření správce front, který používá alternativní skupinu zabezpečení v konfiguraci domény, je vyžadován uživatel domény. Nestačí, aby ID uživatele bylo administrátorem, ačkoli má administrátor oprávnění ke spuštění příkazu **crtmqm** . Uživatel domény, který může být administrátor, musí být členem lokální skupiny mqm a také alternativní skupiny zabezpečení.

V tomto příkladu vytvoříte *wmquser1* a *wmquser2* členy globální skupiny Domain mqm . Průvodce "Příprava produktu IBM MQ " automaticky nakonfiguruje Domain mqm jako člena lokální skupiny mqm , kde se průvodce spustí.

Chcete-li spustit službu IBM MQ pro každou instalaci produktu IBM MQ na jednom počítači, musíte zadat jiného uživatele. Stejně uživatele můžete znovu použít na různých počítačích.

- Ve stromu navigace správce serveru klepněte na nabídku **Uživatelé > Nový > Uživatel** .
 - V okně Nový objekt-Uživatel zadejte *wmquser1* do pole **Přihlašovací jméno uživatele** . Do pole **Křestní jméno** zadejte *WebSphere* a do pole **Příjmení** zadejte *MQ1* . Klepněte na tlačítko **Další** .
 - Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a zrušte označení zaškrťovacího políčka **Uživatel musí změnit heslo při příštím přihlášení** . Klepněte na tlačítko **Další > Dokončit** .
 - V okně Users klepněte pravým tlačítkem myši na **WebSphere MQ > Přidat do skupiny** Zadejte Domain mqm a klepněte na **Zkontrolovat názvy > OK > OK** .
 - Opakujte kroky a až d , chcete-li přidat *WebSphere MQ2* jako *wmquser2* .
15. Spuštění IBM MQ jako služby.

Pokud potřebujete spustit produkt IBM MQ jako službu a poté poskytnout uživateli domény (který jste získali od administrátora domény) přístup ke službě jako službu, proveďte následující postup:

- Klepněte na tlačítko **Start > Spustit**
Zadejte příkaz `secpol . msc` a klepněte na tlačítko **OK** .
- Otevřete **Nastavení zabezpečení > Lokální zásady > Přiřazení uživatelských práv** .
V seznamu zásad klepněte pravým tlačítkem myši na **Přihlásit se jako služba > Vlastnosti** .
- Klepněte na volbu **Přidat uživatele nebo skupinu ...**
Zadejte jméno uživatele, kterého jste získali od administrátora domény, a klepněte na **Kontrolovat názvy** .
- Budete-li vyzváni oknem Zabezpečení produktu Windows , zadejte jméno uživatele a heslo účtu uživatele nebo administrátora účtu s dostatečným oprávněním a klepněte na tlačítko **OK > Použít > OK** .
Zavřete okno Lokální zásada zabezpečení.

Poznámka: Na serveru Windows Server 2008 a Windows Server 2012 je funkce UAC (User Account Control) povolena standardně.

Funkce UAC omezuje akce, které mohou uživatelé provádět na určitých zařízeních operačního systému, i když jsou členy skupiny Administrátoři. Musíte provést příslušné kroky, abyste tato omezení překonali.

Jak pokračovat dále

Pokračujte k další úloze [“Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 413](#).

Související úlohy

[Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows](#)

[Vytvoření sdíleného adresáře pro data správce front a soubory protokolu](#)

Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení

Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows

V této úloze nainstalujete a nakonfigurujete produkt IBM MQ na serveru nebo pracovní stanici v doméně *wmq.example.com* Windows .

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun

Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com* , která obsahuje *Sun* , *mars* a *venus* . Pro účely ilustrace se používá také jako souborový server.

mars

Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR* .

venus

Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR* .

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li vytvořit řadič domény, *sun* pro doménu *wmq.example.com* , proveďte kroky v části [“Vytvoření Active Directory a domény DNS pro IBM MQ”](#) na stránce 409 . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
2. Informace o dalších verzích produktu Windows , na kterých lze spustit produkt IBM MQ , najdete v tématu [Hardwarové a softwarové požadavky na systémech Windows](#) .

Informace o této úloze

V této úloze nakonfigurujete server Windows Server 2008 s názvem *mars* jako člen domény *wmq.example.com* . Nainstalujte produkt IBM MQ a nakonfigurujte instalaci tak, aby se spouštěla jako člen domény *wmq.example.com* .

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolů uložených v adresáři dle vaší volby. Jsou připojeny k úloze, [“Windows domén a správců front s více instancemi”](#) na stránce 405.

Pro účely úlohy je název hostitele řadiče domény *sun* a tyto dva servery IBM MQ se nazývají *mars* a *venus* . Doména se nazývá *wmq.example.com* . Všechny kurzívy v úloze můžete nahradit názvy dle vlastního výběru.

Postup

1. Přidejte řadič domény, *sun.wmq.example.com* do *mars* jako server DNS.
 - a) V produktu *mars* se přihlaste jako *mars\Administrator* a klepněte na tlačítko **Spustit**.
 - b) Klepněte pravým tlačítkem myši na **Síť > Vlastnosti > Spravovat síťová připojení**.
 - c) Klepněte pravým tlačítkem myši na síťový adaptér a poté klepněte na volbu **Vlastnosti**.

System odpoví v okně Vlastnosti připojení k místní síti, které uvádí položky, které připojení používá.
 - d) Ze seznamu položek v okně Vlastnosti připojení lokální oblasti vyberte ze seznamu položek **Internet Protocol verze 4** nebo **Internet Protocol Verze 6** . Klepněte na volbu **Vlastnosti > Rozšířené ...** a klepněte na kartu **DNS** .

- e) Pod adresou serveru DNS klepněte na **Přidat**
 - f) Zadejte adresu IP řadiče domény, který je také serverem DNS, a klepněte na tlačítko **Přidat**.
 - g) Klepněte na volbu **Připojit tyto přípony systému DNS > Přidat**
 - h) Zadejte *wmq.example.com* a klepněte na **Přidat**.
 - i) Zadejte *wmq.example.com* do pole **Přípona systému DNS pro toto připojení**.
 - j) Vyberte volbu **Registrovat tuto adresu připojení v DNS a Použít příponu tohoto připojení v registraci DNS**. Klepněte na tlačítko **OK > OK > Zavřít**.
 - k) Otevřete příkazové okno a zadejte příkaz **ipconfig /all**, abyste zkontrolovali nastavení TCP/IP.
2. V systému *mars* přidejte počítač do domény *wmq.example.com*.
- a) Klepněte na tlačítko **Spustit**
 - b) Klepněte pravým tlačítkem myši na **Počítač > Vlastnosti**. V části **Název počítače, domény a nastavení pracovní skupiny** klepněte na volbu **Změnit nastavení**.
 - c) V oknech vlastností systému klepněte na tlačítko **Změnit**
 - d) Klepněte na doménu, zadejte *wmq.example.com* a klepněte na **OK**.
 - e) Zadejte **Jméno uživatele** a **Heslo** administrátora řadiče domény, který má oprávnění k povolení k připojení počítače k doméně, a klepněte na tlačítko **OK**.
 - f) Klepněte na tlačítko **OK > OK > Zavřít > Restartovat nyní** v odpovědi na zprávu "Vítejte v doméně *wmq.example.com*".
3. Zkontrolujte, zda je počítač členem domény *wmq.example.com*
- a) V systému *sun* se přihlaste k řadiči domény jako *wmq\Administrator*.
 - b) Otevřete produkt **Server Manager > Active Directory Domain Services > wmq.example.com > Počítače** a zkontrolujte, zda je v okně **Počítače** správně uveden *mars*.
4. Nainstalujte IBM MQ for Windows na *mars*.
- Další informace o spuštění průvodce instalací produktu IBM MQ for Windows naleznete v tématu [Instalace serveru IBM MQ v systému Windows](#).
- a) V systému *mars* se přihlaste jako lokální administrátor, *mars\Administrator*.
 - b) Spustěte příkaz **Setup** na instalačním médiu produktu IBM MQ for Windows.
Spustí se příruční panel produktu IBM MQ.
 - c) Klepněte na **Softwarové požadavky**, chcete-li zkontrolovat, zda je nainstalován předem vyžadovaný software.
 - d) Klepněte na **Konfigurace sítě > Ano**, chcete-li konfigurovat ID uživatele domény.
Úloha, "[Vytvoření Active Directory a domény DNS pro IBM MQ](#)" na stránce 409, konfiguruje ID uživatele domény pro tuto sadu úloh.
 - e) Klepněte na volbu **IBM MQ Instalace**, vyberte jazyk instalace a klepněte na volbu **Spustit instalační program** produktu IBM MQ.
 - f) Potvrďte licenční smlouvu a klepněte na tlačítko **Další > Další > Instalovat**, chcete-li přijmout výchozí konfiguraci. Čekajte, až se instalace dokončí, a klepněte na tlačítko **Dokončit**.
Možná budete chtít změnit název instalace, instalovat různé komponenty, konfigurovat jiný adresář pro data správce front a protokoly nebo instalovat do jiného adresáře. Pokud ano, klepněte na volbu **Vlastní** namísto volby **Typická**.
Produkt IBM MQ je instalován a instalační program spustí průvodce "Příprava produktu IBM MQ".
Důležité: Ještě nespouštějte průvodce.
5. Nakonfigurujte uživatele, který bude spouštět službu IBM MQ se správnou volbou **Spustit jako služba**.
- Vyberte, zda chcete konfigurovat lokální skupinu *mqm*, skupinu *Domain mqm* nebo uživatele, který bude spouštět službu IBM MQ se správnou hodnotou. V tomto příkladu dáte uživateli právo.

- a) Klepněte na nabídku **Start > Spustit ...**, Zadejte příkaz **secpol.msc** a klepněte na **OK**.
 - b) Otevřete **Nastavení zabezpečení > Lokální zásady > Přiřazení uživatelských práv**. V seznamu zásad klepněte pravým tlačítkem myši na **Přihlásit se jako služba > Vlastnosti**.
 - c) Klepněte na volbu **Přidat uživatele nebo skupinu ...** a zadejte *wmquser1* a klepněte na **Kontrolovat názvy**
 - d) Zadejte jméno uživatele a heslo administrátora domény, *wmq\Administrátora* klepněte na tlačítko **OK > Použít > OK**. Zavřete okno Lokální zásada zabezpečení.
6. Spusťte průvodce "Příprava produktu IBM MQ " .

Další informace o spuštění průvodce "Příprava produktu IBM MQ " naleznete v tématu [Konfigurace prostoru IBM MQ pomocí Průvodce přípravou produktu IBM MQ](#).

- a) Instalačnímu programu IBM MQ se automaticky spustí "Příprava produktu IBM MQ " .
 Chcete-li průvodce spustit ručně, najděte zástupce složky "Prepare IBM MQ " ve složce **Start > Všechny programy > IBM MQ** . Vyberte zástupce, který odpovídá instalaci produktu IBM MQ v konfiguraci s více instalačními programy.
- b) Klepněte na tlačítko **Další** a v odpovědi na otázku "Označit, zda existuje řadič domény Windows 2000 nebo novější v síti", klepněte na tlačítko **Ano** .
- c) Klepněte na tlačítko **Ano > Další** v okně první konfigurace produktu IBM MQ for Windows pro uživatele domény produktu Windows .
- d) V druhém okně Konfigurace IBM MQ for Windows pro uživatele domény Windows zadejte *wmq* do pole **Doména** . Zadejte *wmquser1* do pole **Jméno uživatele** a heslo, pokud jste jej nastavili, v poli **Heslo** . Klepněte na tlačítko **Další**.
 Průvodce konfiguruje a spouští produkt IBM MQ s parametrem *wmquser1*.
- e) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí zaškrťovacích políček podle potřeby a klepněte na tlačítko **Dokončit**.

Jak pokračovat dále

1. Proved'te úlohu "[Čtení a zápis dat a souborů protokolu registrovaných lokální skupinou produktu mqm](#)" na stránce 436, abyste ověřili, že instalace a konfigurace fungují správně.
2. Proved'te úlohu "[Vytvoření sdíleného adresáře pro data správce front a soubory protokolu](#)" na stránce 415, chcete-li konfigurovat sdílení souborů pro ukládání dat a souborů protokolu správce front s více instancemi.

Související úlohy

[Vytvoření Active Directory a domény DNS pro IBM MQ](#)

[Vytvoření sdíleného adresáře pro data správce front a soubory protokolu](#)

[Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení](#)

Související informace

[Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service](#)

Vytvoření sdíleného adresáře pro data správce front a soubory protokolu

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolů uložených v adresáři dle vaší volby.

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun

Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com* , která obsahuje *Sun* , *mars* a *venus* . Pro účely ilustrace se používá také jako souborový server.

mars

Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR* .

venus

Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR* .

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li provést tuto úlohu přesně podle popisu, proveďte kroky v úloze “Vytvoření Active Directory a domény DNS pro IBM MQ” na stránce 409, chcete-li vytvořit doménu *sun.wmq.example.com* na řadiči domény *sun* . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.

Informace o této úloze

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolů uložených v adresáři dle vaší volby. Jsou připojeny k úloze, “Windows domén a správců front s více instancemi” na stránce 405.

V rámci úlohy vytvoříte sdílení obsahující data a adresář protokolu a globální skupinu pro autorizaci přístupu ke sdílení. Předáte název globální skupiny, která autorizuje podíl na příkazu **crtmqm** ve svém parametru *-a* . Globální skupina vám poskytuje flexibilitu oddělování uživatelů tohoto sdílení od uživatelů jiných sdílených prostředků. Nepotřebujete-li tuto flexibilitu, autorizujte ji raději se skupinou *Domain mqm* , než vytvoříte novou globální skupinu.

Globální skupina použitá pro sdílení v této úloze se nazývá *wmqha* , a sdílení se nazývá *wmq* . Jsou definovány na řadiči domény *sun* v doméně Windows *wmq.example.com* . Podíl má úplná oprávnění k řízení pro globální skupinu *wmqha* . Zaměňte názvy kurzívou v úloze s názvy dle vašeho výběru.

Pro účely této úlohy je řadičem domény stejný server jako souborový server. V praktických aplikacích rozdělte adresář a souborové služby mezi různými servery pro výkon a dostupnost.

Musíte nakonfigurovat ID uživatele, pod kterým je spuštěn správce front, aby byl členem dvou skupin. Musí se jednat o člena lokální skupiny *mqm* na serveru IBM MQ a globální skupině *wmqha* .

Je-li správce front spuštěn jako služba v této sadě úloh, je spuštěn pod ID uživatele *wmquser1* , takže *wmquser1* musí být členem *wmqha* . Je-li správce front spuštěn interaktivně, spustí se pod ID uživatele *wmquser2* , takže *wmquser2* musí být členem *wmqha* . Jak *wmquser1* , tak *wmquser2* jsou členy globální skupiny *Domain mqm*. *Domain mqm* je členem lokální skupiny *mqm* na serverech *mars* a *venus* IBM MQ . Proto jsou *wmquser1* a *wmquser2* členy lokální skupiny *mqm* na obou serverech IBM MQ .

Postup

1. Přihlaste se k řadiči domény, *sun.wmq.example.com* jako administrátor domény.
2. Vytvořte globální skupinu *wmqha* .
 - a) Otevřete produkt **Server Manager** > **Role** > **Active Directory Domain Services** > **wmq.example.com** > **Users**.
 - b) Otevřete složku *wmq.example.com\Users* .
 - c) Klepněte pravým tlačítkem myši na nabídku **Uživatelé** > **Nová** > **Skupina**.
 - d) Zadejte *wmqha* do pole **Název skupiny** .
 - e) Ponechte **Globální** klepnuto jako **Rozsah skupiny** a **Zabezpečení** jako **Typ skupiny**. Klepněte na tlačítko **OK**.

3. Přidejte uživatele domény *wmqluser1* a *wmqluser2* do globální skupiny, *wmqha* .
 - a) Ve stromu navigace správce serveru klepněte na volbu **Uživatelé** a klepněte pravým tlačítkem myši na položku **wmqha > Vlastnosti** v seznamu uživatelů.
 - b) Klepněte na kartu Členové v okně Vlastnosti *wmqha* .
 - c) Klepněte na tlačítko **Přidat ...** ; napište *wmqluser1* ; *wmqluser2* a klepněte na **Zkontrolovat názvy > OK > Použít > OK**.
4. Vytvořte adresářový strom, který bude obsahovat data správce front a soubory protokolu.
 - a) Otevřete příkazový řádek.
 - b) Zadejte příkaz:

```
md c:\wmq\data, c:\wmq\logs
```

5. Autorizujte globální skupinu *wmqha* , aby měla oprávnění k úplnému řízení pro adresáře a sdílení produktu *c:\wmq* .
 - a) V produktu Windows Explorer klepněte pravým tlačítkem myši na **c:\wmq > Vlastnosti**.
 - b) Klepněte na kartu **Zabezpečení** a klepněte na volbu **Rozšířené > Upravit ...**
 - c) Zrušte označení zaškrtačacího políčka **Zahrnout oprávnění k dědičné oprávnění u vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení produktu Windows .
 - d) Vyberte řádky pro uživatele v seznamu **Položky oprávnění** a klepněte na tlačítko **Odebrat**. Řádky pro SYSTEM, Administrators a CREATOR OWNER ponechejte v seznamu **Položky oprávnění**.
 - e) Klepněte na tlačítko **Přidat ...** a zadejte název globální skupiny *wmqha* . Klepněte na volbu **Zkontrolovat názvy > OK**.
 - f) V okně Položka oprávnění pro *wmq* vyberte **Úplné řízení** v seznamu **Oprávnění**.
 - g) Klepněte na tlačítko **OK > Použít > OK > OK > OK**
 - h) V produktu Windows Explorer klepněte pravým tlačítkem myši na **c:\wmq > Sdílet ...**
 - i) Klepněte na volbu **Rozšířené sdílení ...** a vyberte zaškrtačací políčko **Sdílet tuto složku** . Název sdílení ponechte jako *wmq* .
 - j) Klepněte na volbu **Oprávnění > Přidat ...**, a zadejte název globální skupiny *wmqha* . Klepněte na volbu **Zkontrolovat názvy > OK**.
 - k) Vyberte položku *wmqha* v seznamu **Názvy skupin nebo uživatelů**. Označte zaškrtačací políčko **Úplné řízení** v seznamu **Oprávnění pro wmqha** ; klepněte na tlačítko **Použít**.
 - l) Vyberte položku *Administrators* v seznamu **Názvy skupin nebo uživatelů**. Vyberte zaškrtačací políčko **Úplné řízení** v seznamu **Oprávnění pro Administrátoři** . klepněte na tlačítko **Použít > OK > OK > Zavřít**.

Jak pokračovat dále

Zkontrolujte, zda je možné číst a zapisovat soubory do sdílených adresářů z každého ze serverů IBM MQ . Zkontrolujte ID uživatele služby IBM MQ , *wmqluser1* a interaktivní ID uživatele *wmqluser2*.

1. Používáte-li vzdálenou pracovní plochu, musíte přidat *wmq\wmqluser1* a *wmqluser2* do lokální skupiny Remote Desktop Users na *mars* .
 - a. Přihlaste se k produktu *mars* jako *wmq\Administrator*
 - b. Spuštěním příkazu **lusrmgr.msc** otevřete okno Lokální uživatelé a skupiny.
 - c. Klepněte na volbu **Skupiny**. Klepněte pravým tlačítkem myši na volbu **Uživatelé vzdálené pracovní plochy > Vlastnosti > Přidat ...** Zadejte *wmqluser1* ; *wmqluser2* a klepněte na **Kontrolovat názvy**.
 - d. Zadejte jméno uživatele a heslo administrátora domény, *wmq\Administratora* klepněte na tlačítko **OK > Použít > OK**.
 - e. Zavřete okno Lokální uživatelé a skupiny.

2. Přihlaste se k produktu *mars* jako *wmq\wmquser1*.
 - a. Otevřete okno produktu Windows Explorer a zadejte příkaz `\\sun\wmq` .

System odpoví otevřením podílu portálu *wmq* na systému *sun.wmq.example.com* a vypíše seznam adresářů dat a protokolů.
 - b. Zkontrolujte oprávnění produktu *wmquser1* tak, že vytvoříte soubor v podadresáři dat, přidáte nějaký obsah, že jej budete číst a pak jej vymažete.
3. Přihlaste se k produktu *mars* jako *wmq\wmquser2* a zopakujte kontrolu.
4. Proveďte další úlohu, abyste vytvořili správce front pro použití sdílených dat a adresářů protokolu, viz “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 418.

Související úlohy

Vytvoření Active Directory a domény DNS pro IBM MQ

Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows

Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení

Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení

Tato úloha ukazuje, jak použít parametr `-a` u příkazu **`crtmqm`**. Příznak `-a` poskytuje správci front přístup k svým protokolovým souborům a datovým souborům ve vzdáleném sdílení souborů pomocí alternativní skupiny zabezpečení.

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun

Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com*, která obsahuje *Sun*, *mars* a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars

Server Windows Server 2008 použitý jako první server IBM MQ. Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus

Server Windows Server 2008 používaný jako druhý server IBM MQ. Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

Postupujte podle kroků uvedených v následujících úlohách. Úlohy vytvoří řadič domény a doménu, nainstalujete produkt IBM MQ for Windows na jeden server a vytvoříte sdílení souboru pro data a soubory protokolu. Pokud konfiguruje existující řadič domény, můžete zjistit, že je užitečné vyzkoušet si kroky na novém serveru Windows Server 2008. Kroky je možné upravit podle své domény.

1. “Vytvoření Active Directory a domény DNS pro IBM MQ” na stránce 409.
2. “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 413.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu” na stránce 415.

Informace o této úloze

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolu

uložených v adresáři dle vaší volby. Jsou připojeny k úloze, “Windows domén a správců front s více instancemi” na stránce 405.

V této úloze vytvoříte správce front, ve kterém jsou uložena data a protokoly ve vzdáleném adresáři na souborovém serveru. Pro účely tohoto příkladu je souborový server stejným serverem jako řadič domény. Adresář obsahující data a složky protokolu je sdílen s úplným oprávněním pro řízení, které je poskytnuto globální skupině `wmqha`.

Postup

1. Přihlaste se k serveru domény, `mars` jako lokální administrátor, `mars\Administrator`.
2. Otevřte příkazové okno.
3. Restartujte službu IBM MQ .

Musíte restartovat službu, aby ID uživatele, pod kterým je spuštěna, získá přídavná pověření zabezpečení, která jste pro něj nakonfigurovali.

Zadejte příkazy:

```
endmqsvc  
strmqsvc
```

Systémové odezvy:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.  
The MQ service for installation 'Installation1' ended successfully.
```

A:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.  
The MQ service for installation 'Installation1' started successfully.
```

4. Vytvořte správce front.

```
crtmqm -a wmq\wmqha -sax -u SYSTEM.DEAD.LETTER.QUEUE -md \\sun\wmq\data -ld \\sun\wmq\logs  
QMGR
```

Musíte zadat doménu, `wmq` , alternativní skupiny zabezpečení `wmqha` uvedením úplného názvu domény globální skupiny `"wmq\wmqha"` .

Musíte vyhláskovat název UNC (Universal Naming Convention) pro sdílení `\\sun\wmq` a nepoužívat odkaz na mapovaný disk.

Odezva systému:

```
IBM MQ queue manager created.  
Directory '\\sun\wmq\data\QMGR' created.  
The queue manager is associated with installation '1'  
Creating or replacing default objects for queue manager 'QMGR'  
Default objects statistics : 74 created. 0 replaced.  
Completing setup.  
Setup completed.
```

Jak pokračovat dále

Otestujte správce front tak, že do fronty vložíte zprávu do fronty.

1. Spusťte správce front.

```
strmqm QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.  
The queue manager is associated with installation '1'.  
5 log records accessed on queue manager 'QMGR' during the log  
replay phase.  
Log replay for queue manager 'QMGR' complete.  
Transaction manager state recovered for queue manager 'QMGR'.  
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

2. Vytvořte testovací frontu.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

Odezva systému:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.  
Starting MQSC for queue manager QMGR.
```

```
1 : define qlocal(QTEST)  
AMQ8006: IBM MQ queue created.  
One MQSC command read.  
No commands have a syntax error.  
All valid MQSC commands were processed.
```

3. Vložte testovací zprávu pomocí ukázkového programu **amqsput**.

```
echo 'A test message' | amqsput QTEST QMGR
```

Odezva systému:

```
Sample AMQSPUT0 start  
target queue is QTEST  
Sample AMQSPUT0 end
```

4. Získejte testovací zprávu pomocí ukázkového programu **amqsget**.

```
amqsget QTEST QMGR
```

Odezva systému:

```
Sample AMQSGET0 start  
message <A test message>  
Wait 15 seconds ...  
no more messages  
Sample AMQSGET0 end
```

5. Zastavte správce front.

```
endmqm -i QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

Tip: Přidejte do příkazů volbu /Q , abyste zabránili příkazu, aby se vymazal každý soubor nebo adresář.

```
del /F /S C:\wmq\*.*  
rmdir /S C:\wmq
```

Související úlohy

[Vytvoření Active Directory a domény DNS pro IBM MQ](#)

[Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows](#)

[Vytvoření sdíleného adresáře pro data správce front a soubory protokolu](#)

Vytvoření správce front s více instancemi na řadičích domény

Příklad ukazuje, jak nastavit správce front s více instancemi na Windows na řadičích domény. Nastavení demonstruje zahrnuté koncepce, spíše než aby bylo produkční měřítko. Tento příklad je založen na serveru Windows Server 2008. Tyto kroky se mohou lišit od dalších verzí serveru Windows .

Konfigurace používá koncept mini-domény nebo "domainlet" ; Viz uzly klastru Windows 2000, Windows Server 2003 a Windows Server 2008 jako řadiče domény. Chcete-li do existující domény přidat správce front s více instancemi, přečtěte si téma "[Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény](#)" na stránce 406.

Příklad konfigurace se skládá ze tří serverů:

sun

Server Windows Server 2008 používaný jako první řadič domény. Definuje doménu *wmq.example.com* , která obsahuje *sun* , *earth* a *mars* . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR* .

earth

Server Windows Server 2008 používaný jako druhý server řadiče domény IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR* .

mars

Server Windows Server 2008 používaný jako souborový server.

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. V systému Windows není nutné ověřovat systém souborů, do kterého chcete ukládat data správce front a soubory žurnálu. Procedura kontroly, [Ověření chování sdíleného systému souborů](#), je použitelná pro SYSTÉM UNIX a Linux. V systému Windows jsou kontroly vždy úspěšné.
2. Chcete-li vytvořit první řadič domény, proveďte kroky v části "[Vytvoření Active Directory a domény DNS pro IBM MQ](#)" na stránce 409 .
3. Chcete-li přidat druhý řadič domény, nainstalujte produkt IBM MQ for Windows na oba řadiče domény a ověřte instalaci pomocí kroků uvedených v tématu "[Přidání druhého řadiče domény do domény wmq.example.com](#) " na stránce 425 .

4. Proveďte kroky uvedené v části [“Instalace produktu IBM MQ na řadičích domény v doméně `wmq.example.com`”](#) na stránce 426 a nainstalujte produkt IBM MQ na dva řadiče domény.

Informace o této úloze

Na souborovém serveru ve stejné doméně vytvořte sdílené adresáře pro protokol správce front a datové adresáře. Dále vytvořte první instanci správce front s více instancemi, který používá sdílení souboru na jednom z řadičů domény. Vytvořte druhou instanci na jiném řadiči domény a nakonec ověřte konfiguraci. Můžete vytvořit sdílení souboru na řadiči domény.

V ukázce je *sun* prvním řadičem domény, *earth* druhým a *mars* je souborový server.

Postup

1. Vytvořte adresáře, které budou obsahovat data správce front a soubory protokolu.

a) V systému *mars* zadejte příkaz:

```
md c:\wmq\data , c:\wmq\logs
```

2. Sdílejte adresáře, které mají obsahovat data správce front a soubory protokolu.

Musíte povolit úplný přístup k řízení přístupu k lokální skupině domén *mqma* ID uživatele, které používáte k vytvoření správce front. V tomto příkladu mají ID uživatelů, kteří jsou členy produktu *Domain Administrators*, oprávnění k vytváření správců front.

Sdílení souboru musí být na serveru, který je ve stejné doméně jako řadiče domény. V tomto příkladě je server *mars* ve stejné doméně jako řadiče domény.

- a) V produktu Windows Explorer klepněte pravým tlačítkem myši na **c: \wmq > Vlastnosti**.
- b) Klepněte na kartu **Zabezpečení** a klepněte na volbu **Rozšířené > Upravit ...**
- c) Zrušte označení zaškrtačícího políčka **Zahrnout oprávnění k dědičné oprávnění u vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení produktu Windows .
- d) Vyberte řádky pro uživatele v seznamu **Položky oprávnění** a klepněte na tlačítko **Odebrat**. Řádky pro **SYSTEM**, **Administrators** a **CREATOR OWNER** ponechejte v seznamu **Položky oprávnění**.
- e) Klepněte na tlačítko **Přidat ...** a zadejte název lokální skupiny domén *mqm* . Klepněte na **Kontrolovat názvy**
- f) Jako odpověď na okno zabezpečení produktu Windows zadejte název a heslo produktu *Domain Administrator* a klepněte na tlačítko **OK > OK**.
- g) V okně **Položka oprávnění** pro *wmq* vyberte **Úplné řízení** v seznamu **Oprávnění**.
- h) Klepněte na tlačítko **OK > Použít > OK > OK > OK**
- i) Opakujte kroky **e** až **h**, chcete-li přidat *Domain Administrators*.
- j) V produktu Windows Explorer klepněte pravým tlačítkem myši na **c: \wmq > Sdílet ...**
- k) Klepněte na volbu **Rozšířené sdílení ...** a vyberte zaškrtačící políčko **Sdílet tuto složku** . Název sdílení ponechte jako *wmq* .
- l) Klepněte na volbu **Oprávnění > Přidat ...**, a zadejte název lokální skupiny domén *mqm* ; *Domain Administrators*. Klepněte na volbu **Kontrolovat názvy**.
- m) Jako odpověď na okno zabezpečení produktu Windows zadejte název a heslo produktu *Domain Administrator* a klepněte na tlačítko **OK > OK**.
3. Vytvořte správce front *QMGR* na prvním řadiči domény *sun* .

```
crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md \\mars\wmq\data -ld \\mars\wmq\logs QMGR
```

Odezva systému:

```
IBM MQ queue manager created.
Directory '\\mars\wmq\data\QMGR' created.
The queue manager is associated with installation 'Installation1'.
Creating or replacing default objects for queue manager 'QMGR'.
Default objects statistics : 74 created. 0 replaced. 0 failed.
Completing setup.
Setup completed.
```

4. Spusťte správce front v systému *sun* tak, že povolíte instanci v pohotovostním režimu.

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

5. Vytvořte druhou instanci produktu *QMGR* v systému *earth* .
- a) Zkontrolujte hodnoty parametrů *Předpona* a *InstallationName* , které jsou správné pro produkt *earth* .

V systému *sun* spusťte příkaz **dspmqinf** :

```
dspmqinf QMGR
```

Odezva systému:

```
QueueManager:
Name=QMGR
Directory=QMGR
Prefix=C:\ProgramData\IBM\MQ
DataPath=\\mars\wmq\data\QMGR
InstallationName=Installation1
```

- b) Okopírujte strojově čitelnou formu stanzy **QueueManager** do schránky.

V systému *sun* spusťte příkaz **dspmqinf** znovu s parametrem `-o command` .

```
dspmqinf -o command QMGR
```

Odezva systému:

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\mars\wmq\data\QMGR
```

- c) V systému *earth* spusťte příkaz **addmqinf** ze schránky a vytvořte instanci správce front v systému *earth* .

V případě potřeby upravte příkaz tak, aby vyhovoval rozdílům v parametrech Předpona nebo InstallationName .

```
addmqinf -s QueueManager -v Name= QMGR
-v Directory= QMGR -v Prefix="C:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\mars\wmq\data\QMGR
```

IBM MQ configuration information added.

6. Spusťte instanci v pohotovostním režimu správce front v systému *earth* .

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
A standby instance of queue manager 'QMGR' has been started. The active
instance is running elsewhere.
```

Výsledky

Ověřte, zda se správce front přepne z *sun* na *earth* :

1. V systému *sun* spusťte příkaz:

```
endmqm -i -r -s QMGR
```

Odezva systému na *sun* :

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended, permitting switchover to
a standby instance.
```

2. U *earth* opakovaně zadejte příkaz:

```
dspmq
```

Systémové odezvy:

```
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running)
```

Jak pokračovat dále

Chcete-li ověřit správce front s více instancemi pomocí ukázkových programů, přečtěte si téma [“Ověřte správce front s více instancemi v systému Windows”](#) na stránce 429.

Související úlohy

[“Přidání druhého řadiče domény do domény wmq.example.com ”](#) na stránce 425

[“Instalace produktu IBM MQ na řadičích domény v doméně wmq.example.com ”](#) na stránce 426

Související informace

uzly klastru Windows 2000, Windows Server 2003 a Windows Server 2008 jako řadiče domény

Přidání druhého řadiče domény do domény `wmq.example.com`

Přidejte druhý řadič domény do domény `wmq.example.com` za účelem vytvoření domény Windows, ve které se mají spouštět správce front s více instancemi na řadičích domény a na souborových serverech.

Příklad konfigurace se skládá ze tří serverů:

sun

Server Windows Server 2008 používaný jako první řadič domény. Definuje doménu `wmq.example.com`, která obsahuje `sun`, `earth` a `mars`. Obsahuje jednu instanci správce front pro více instancí s názvem `QMGR`.

earth

Server Windows Server 2008 používaný jako druhý server řadiče domény IBM MQ. Obsahuje druhou instanci správce front pro více instancí s názvem `QMGR`.

mars

Server Windows Server 2008 používaný jako souborový server.

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li vytvořit řadič domény, `sun` pro doménu `wmq.example.com`, proveďte kroky v části [“Vytvoření Active Directory a domény DNS pro IBM MQ”](#) na stránce 409. Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
2. Nainstalujte produkt Windows Server 2008 na server ve výchozí pracovní skupině, WORKGROUP. Pro tento příklad je server pojmenován `earth`.

Informace o této úloze

V této úloze nakonfigurujete server Windows Server 2008 s názvem `earth` jako druhý řadič domény v doméně `wmq.example.com`.

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolů uložených v adresáři dle vaší volby. Jsou připojeny k úloze, [“Windows domén a správců front s více instancemi”](#) na stránce 405.

Postup

1. Přidejte řadič domény, `sun.wmq.example.com` do `earth` jako server DNS.
 - a) V produktu `earth` se přihlaste jako `earth\Administrator` a klepněte na tlačítko **Spustit**.
 - b) Klepněte pravým tlačítkem myši na **Síť > Vlastnosti > Spravovat síťová připojení**.
 - c) Klepněte pravým tlačítkem myši na síťový adaptér a poté klepněte na volbu **Vlastnosti**.

System odpoví v okně Vlastnosti připojení k místní síti, které uvádí položky, které připojení používá.
 - d) Ze seznamu položek v okně Vlastnosti připojení lokální oblasti vyberte ze seznamu položek **Internet Protocol verze 4** nebo **Internet Protocol Verze 6**. Klepněte na volbu **Vlastnosti > Rozšířené ...** a klepněte na kartu **DNS**.
 - e) Pod adresou serveru DNS klepněte na **Přidat ...**
 - f) Zadejte adresu IP řadiče domény, který je také serverem DNS, a klepněte na tlačítko **Přidat**.
 - g) Klepněte na volbu **Připojit tyto přípony systému DNS > Přidat ...**
 - h) Zadejte `wmq.example.com` a klepněte na **Přidat**.
 - i) Zadejte `wmq.example.com` do pole **Přípona systému DNS pro toto připojení**.

- j) Vyberte volbu **Registrovat tuto adresu připojení v DNS** a **Použít příponu tohoto připojení v registraci DNS**. Klepněte na tlačítko **OK > OK > Zavřít** .
- k) Otevřete příkazové okno a zadejte příkaz **ipconfig /all** , abyste zkontrolovali nastavení TCP/IP.
2. Přihlaste se k řadiči domény *sun* jako administrátor lokálního systému nebo administrátor produktu Workgroup .
- Je-li server již konfigurován jako řadič domény, musíte se přihlásit jako administrátor domény.
3. Spusťte průvodce Active Directory Domain Services.
- a) Klepněte na nabídku **Start > Spustit ...** Zadejte `dcpromo` a klepněte na **OK**.
Nejsou-li binární soubory Active Directory již nainstalovány, produkt Windows nainstaluje soubory automaticky.
4. Konfigurujte *earth* jako druhý řadič domény v doméně *wmq.example.com* .
- a) V prvním okně průvodce ponechte zaškrtnuté políčko **Použít rozšířenou instalaci režimu** prázdné. Klepněte na tlačítko **Další > Další** a klepněte na volbu **Vytvořit přidat řadič domény do existující domény > Další**.
- b) Zadejte *wmq* do pole **Zadejte název libovolné domény v tomto lese ...** . Klepnete-li na přepínač **Alternativní pověření** , klepněte na **Nastavit ...** Zadejte jméno a heslo administrátora domény a klepněte na tlačítko **OK > Další > Další > Další**.
- c) V okně **Další** volby řadiče domény přijměte volby **Server DNS** a **Globální katalog** , které jste vybrali. Klepněte na tlačítko **Další > Další**.
- d) Na heslo administrátora režimu obnovy adresářových služeb zadejte heslo do polí **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **Další > Další**.
- e) Když jste vyzváni k zadání **Síťových pověření**, zadejte heslo administrátora domény. V závěrečném okně průvodce vyberte volbu **Znovu spustit po dokončení** .
- f) Po nějakou dobu se může okno otevřít s chybou **DCPromo** týkající se delegování DNS; klepněte na tlačítko **OK**. Server znovu zavede systém.

Výsledky

Po opětném zavedení systému *earth* se přihlaste jako administrátor domény. Zkontrolujte, zda byla doména *wmq.example.com* replikována na *earth* .

Jak pokračovat dále

Pokračujte instalací produktu IBM MQ ; viz [“Instalace produktu IBM MQ na řadičích domény v doméně *wmq.example.com*”](#) na stránce 426.

Související úlohy

[Instalace produktu IBM MQ na řadičích domény v doméně *wmq.example.com*](#)
[“Vytvoření Active Directory a domény DNS pro IBM MQ”](#) na stránce 409

*Instalace produktu IBM MQ na řadičích domény v doméně *wmq.example.com**

Nainstalujte a nakonfigurujte instalace produktu IBM MQ na obou řadičích domény v doméně *wmq.example.com* .

Sem zadejte krátký popis; použijte se pro první odstavec a abstrakt.

Příklad konfigurace se skládá ze tří serverů:

sun

Server Windows Server 2008 používaný jako první řadič domény. Definuje doménu *wmq.example.com* , která obsahuje *sun* , *earth* a *mars* . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR* .

earth

Server Windows Server 2008 používaný jako druhý server řadiče domény IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR* .

mars

Server Windows Server 2008 používaný jako souborový server.

Nahradte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li vytvořit řadič domény, *sun* pro doménu *wmq.example.com*, proveďte kroky v části "[Vytvoření Active Directory a domény DNS pro IBM MQ](#)" na stránce 409. Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
2. Chcete-li vytvořit druhý řadič domény, *earth*, pro doménu *wmq.example.com*, proveďte kroky v části "[Přidání druhého řadiče domény do domény wmq.example.com](#)" na stránce 425. Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
3. Informace o dalších verzích produktu Windows, na kterých lze spustit produkt IBM MQ, najdete v tématu [Hardwarové a softwarové požadavky na systémech Windows](#).

Informace o této úloze

Nainstalujte a nakonfigurujte instalace produktu IBM MQ na obou řadičích domény v doméně *wmq.example.com*.

Postup

1. Nainstalujte IBM MQ na *sun* a *earth*.

Další informace o spuštění průvodce instalací produktu IBM MQ for Windows naleznete v tématu [Instalace serveru IBM MQ v systému Windows](#).

- a) V systémech *sun* a *earth* se přihlaste jako administrátor domény *wmq\Administrator*.
- b) Spusťte příkaz **Setup** na instalačním médiu produktu IBM MQ for Windows.

Spustí se příruční panel produktu IBM MQ.

- c) Klepněte na **Softwarové požadavky**, chcete-li zkontrolovat, zda je nainstalován předem vyžadovaný software.
- d) Klepněte na volbu **Konfigurace sítě > Ne**.

Můžete konfigurovat buď ID uživatele domény, nebo ne pro tuto instalaci. ID uživatele, který se vytvoří, je ID lokálního uživatele domény.

- e) Klepněte na volbu **IBM MQ Instalace**, vyberte jazyk instalace a klepněte na volbu Spustit instalační program produktu IBM MQ.

- f) Potvrďte licenční smlouvu a klepněte na tlačítko **Další > Další > Instalovat**, chcete-li přijmout výchozí konfiguraci. Čekejte, až se instalace dokončí, a klepněte na tlačítko **Dokončit**.

Chcete-li změnit název instalace, instalovat různé komponenty, konfigurovat jiný adresář pro data správce front a protokoly nebo instalovat do jiného adresáře, klepněte na volbu **Vlastní** namísto volby **Typická**.

Produkt IBM MQ je instalován a instalační program spustí průvodce "Příprava produktu IBM MQ".

Instalace produktu IBM MQ for Windows nakonfiguruje lokální skupinu domén *mqm* skupinu domén *Domain mqm*. *Domain mqm* je členem *mqm*. Následné řadiče domény ve stejné doméně sdílejí skupinu *mqm* a *Domain mqm*.

2. V produktu *earth* i v produktu *sun* spusťte "Průvodce přípravou produktu IBM MQ".

Další informace o spuštění průvodce "Příprava produktu IBM MQ" naleznete v tématu [Konfigurace portálu IBM MQ pomocí Průvodce přípravou produktu IBM MQ](#).

- a) Instalační program produktu IBM MQ spustí automaticky "Příprava produktu IBM MQ".

Chcete-li průvodce spustit ručně, najdete zástupce složky "Prepare IBM MQ" ve složce **Start** > **Všechny programy** > **IBM MQ**. Vyberte zástupce, který odpovídá instalaci produktu IBM MQ v konfiguraci s více instalačními programy.

- b) Click **Další** and leave **Ne** clicked in response to the question "Identifikujte, zda v síti existuje řadič domény Windows 2000 nebo novější."¹.
- c) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí zaškrťovacích políček podle potřeby a klepněte na tlačítko **Dokončit**.

Průvodce "Příprava produktu IBM MQ" vytvoří doménový lokální uživatel MUSR_MQADMIN na prvním řadiči domény a další lokální uživatele domény MUSR_MQADMIN1 na druhém řadiči domény. Průvodce vytvoří službu IBM MQ na každém řadiči, s MUSR_MQADMIN nebo MUSR_MQADMIN1 jako uživatele, který se přihlásí na službu.

3. Definujte uživatele, který má oprávnění k vytvoření správce front.

Uživatel musí mít právo přihlásit se lokálně a musí být členem lokální skupiny mqm domény. V řadičích domény nemají uživatelé domény právo přihlásit se lokálně, ale administrátoři ano. Při výchozím nastavení nemá žádný uživatel tyto atributy. V této úloze přidejte administrátory domény do lokální skupiny mqm domény.

- a) Otevřete produkt **Server Manager** > **Role** > **Active Directory Domain Services** > **wmq.example.com** > **Users**.
- b) Right-click **Administrátoři domény** > **Přidat do skupiny ...** a typu mqm ; klepněte na volbu **Zkontrolovat názvy** > **OK** > **OK**

Výsledky

1. Zkontrolujte, zda "Prepare IBM MQ" vytvořil uživatele domény, MUSR_MQADMIN:
 - a. Otevřete produkt **Server Manager** > **Role** > **Active Directory Domain Services** > **wmq.example.com** > **Users**.
 - b. Right-click **MUSR_MQADMIN** > **Vlastnosti ...** > **Člena** uvidíte, že se jedná o člena Domain users a mqm.
2. Zkontrolujte, že produkt MUSR_MQADMIN má právo pracovat jako služba:
 - a. Klepněte na nabídku **Start** > **Spustit ...**, Zadejte příkaz **secpol.msc** a klepněte na **OK**.
 - b. Otevřete **Nastavení zabezpečení** > **Lokální zásady** > **Přiřazení uživatelských práv**. V seznamu zásad klepněte pravým tlačítkem myši na **Přihlásit se jako služba** > **Vlastnosti** a viz MUSR_MQADMIN se uvádí jako mající právo přihlásit se jako služba. Klepněte na tlačítko **OK**.

Jak pokračovat dále

1. Provedte úlohu "Čtení a zápis dat a souborů protokolu registrovaných lokální skupinou produktu mqm" na stránce 436, abyste ověřili, že instalace a konfigurace fungují správně.
2. Přejděte zpět na úlohu "Vytvoření správce front s více instancemi na řadičích domény" na stránce 421, abyste dokončili úlohu konfigurace správce front s více instancemi na řadičích domény.

Související úlohy

Přidání druhého řadiče domény do domény wmq.example.com

Související informace

Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service

¹ Můžete nakonfigurovat instalaci pro doménu. Vzhledem k tomu, že všichni uživatelé a skupiny na řadiči domény mají rozsah domény, neodlišujte se tím. Je jednodušší instalovat produkt IBM MQ, jako by se nenachází v doméně.

Ověřte správce front s více instancemi v systému Windows

Chcete-li ověřit konfiguraci správce front s více instancemi, použijte ukázkové programy **amqsgshac**, **amqspshac** a **amqsmhac**. Toto téma nabízí vzorovou konfiguraci pro ověření konfigurace správce front s více instancemi na serveru Windows Server 2003.

Ukázkové programy s vysokou dostupností používají automatické opětovné připojení klienta. Dojde-li k selhání připojeného správce front, klient se pokusí znovu připojit ke správci front ve stejné skupině správců front. Popis ukázek, **ukázkových programů vysoké dostupnosti**, demonstruje opětovné připojení klienta pomocí správce front s jedinou instancí pro zjednodušení. Chcete-li ověřit konfiguraci správce front s více instancemi, můžete použít stejné ukázky s více správci front pro více instancí.

Tento příklad používá konfiguraci s více instancemi popsanou v části **“Vytvoření správce front s více instancemi na řadičích domény”** na stránce 421. Použijte konfiguraci k ověření, že správce front s více instancemi se přepne na instanci v pohotovostním režimu. Zastavte správce front pomocí příkazu **endmqm** a použijte volbu **-s, switchover, option**. Programy klienta se znovu připojí k nové instanci správce front a budou pokračovat v práci s novou instancí po mírném zpoždění.

Klient je instalován v obrazu 400 MB VMware, kde je spuštěn produkt Windows 7 Service Pack 1. Z bezpečnostních důvodů je připojen ke stejné síti hostitele VMware jako servery domén, na kterých běží správce front s více instancemi. Sdílí konfiguraci se složkou /MQHA, která obsahuje tabulku připojení klienta, a zjednodušíte tak konfiguraci.

Ověření překonání selhání pomocí Průzkumníka IBM MQ

Než použijete ukázkové aplikace k ověření překonání selhání, spusťte na každém serveru Průzkumníka IBM MQ. Přidejte obě instance správce front do každého průzkumníku pomocí průvodce **Přidat vzdáleného správce front > Připojit přímo k víceinstanceinstanční správci front**. Ujistěte se, že obě instance jsou spuštěny, což umožňuje pohotovostní režim. Zavřete okno se spuštěnou instancí VMware s aktivní instancí, virtuálně vypněte server nebo zastavte aktivní instanci, což umožňuje přepnutí na záložní instanci a opětovné připojení klientů k opětovnému připojení.

Poznámka: Vypnete-li server, ujistěte se, že se nejedná o adresář, který je hostitelem složky MQHA!

Poznámka: Volba **Povolit přepnutí na instanci v pohotovostním režimu** nemusí být k dispozici v dialogovém okně **Zastavit správce front**. Volba chybí, protože správce front je spuštěn jako správce front s jednou instancí. Musíte je spustit bez volby **Povolit instanci v pohotovostním režimu**. Pokud je váš požadavek na zastavení správce front odmítnut, podívejte se do okna **Podrobnosti**, pravděpodobně není spuštěna žádná instance v pohotovostním režimu.

Ověření překonání selhání pomocí ukázkových programů

Zvolte server, na kterém má být spuštěna aktivní instance.

Je možné, že jste zvolili jeden ze serverů pro hostování adresáře MQHA nebo systému souborů. Pokud plánujete otestovat překonání selhání zavřením okna VMware se spuštěným aktivním serverem, ujistěte se, že to není ten, který hostuje MQHA!

Na serveru, na kterém je spuštěna aktivní instance správce front

1. Upravte hodnoty *ipaddr1* a *ipaddr2* a uložte následující příkazy v produktu N:\hasample.tst. .

```
DEFINE QLOCAL(SOURCE) REPLACE
DEFINE QLOCAL(TARGET) REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(SVRCONN) TRPTYPE(TCP) +
MCAUSER(' ') REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNNAME(' ipaddr1 (1414), ipaddr2 (1414)') QMNAME(QM1) REPLACE
START CHANNEL(CHANNEL1)
DEFINE LISTENER(LISTENER.TCP) TRPTYPE(TCP) CONTROL(QMGR)
DISPLAY LISTENER(LISTENER.TCP) CONTROL
DISPLAY LSSTATUS(LISTENER.TCP) STATUS
```

Poznámka: Pokud ponecháte parametr **MCAUSER** prázdný, odešle se klientovi ID uživatele klienta. ID uživatele klienta musí mít na serverech správná oprávnění. Alternativou je nastavit parametr **MCAUSER** v kanálu SVRCONN na ID uživatele, které jste nakonfigurovali na serveru.

2. Otevřete příkazový řádek s cestou N: \ a spusťte příkaz:

```
runmqsc -m QM1 < hasample.tst
```

3. Ověřte, zda je modul listener spuštěný a má-li řízení správce front, a to buď kontrolou výstupu příkazu **runmqsc** .

```
LISTENER(LISTENER.TCP)CONTROL(QMGR)  
LISTENER(LISTENER.TCP)STATUS(RUNNING)
```

Nebo pomocí Průzkumníka IBM MQ , že je spuštěn modul listener protokolu TCP/IP, a má Control = Queue Manager.

Na klientu

1. Namapujte sdílený adresář C : \MQHA na serveru na N : \ na straně klienta.
2. Otevřete příkazový řádek s cestou N : \ . Nastavte proměnnou prostředí MQCHLLIB tak, aby ukazovala na tabulku definic kanálů klienta (CCDT) na serveru:

```
SET MQCHLLIB=N:\data\QM1\@ipcc
```

3. Na příkazový řádek zadejte příkazy:

```
start amqsghac TARGET QM1  
start amqsmhac -s SOURCE -t TARGET -m QM1  
start amqsphac SOURCE QM1
```

Poznámka: Máte-li problémy, spusťte aplikace na příkazovém řádku tak, aby kód příčiny byl vytištěn na konzole, nebo se podívejte na AMQERR01.LOG ve složce N : \data\QM1\errors .

Na serveru, na kterém je spuštěna aktivní instance správce front

1. Proved'te jednu z následujících akcí:
 - Zavřete okno se spuštěnou instancí serveru VMware s obrazem aktivního serveru.
 - Pomocí Průzkumníka IBM MQ zastavte aktivní instanci správce front, což umožňuje přepnutí do instance v pohotovostním režimu a instruující se znovu připojitelné klienty k opětovnému připojení.
2. Tři klienti nakonec zjistí, že spojení je přerušeno, a pak se znovu připojí. V této konfiguraci, pokud zavřete okno serveru, trvá přibližně sedm minut, než se znovu ustanoví všechna tři připojení. Někteří spojení se znovu ustanoví dobře před ostatními.

Výsledky

```
N:\>amqsphac SOURCE QM1  
Sample AMQSPHAC start  
target queue is SOURCE  
message <Message 1>  
message <Message 2>  
message <Message 3>  
message <Message 4>  
message <Message 5>  
17:05:25 : EVENT : Connection Reconnecting (Delay: 0ms)  
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)  
17:05:52 : EVENT : Connection Reconnected  
message <Message 6>  
message <Message 7>  
message <Message 8>  
message <Message 9>
```

```
N:\>amqsmhac -s SOURCE -t TARGET -m QM1
Sample AMQSMHA0 start
```

```
17:05:25 : EVENT : Connection Reconnecting (Delay: 97ms)
17:05:48 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:53 : EVENT : Connection Reconnected
```

```
N:\>amqsgnac TARGET QM1
Sample AMQSGHAC start
message <Message 1>
message <Message 2>
message <Message 3>
message <Message 4>
message <Message 5>
17:05:25 : EVENT : Connection Reconnecting (Delay: 156ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message <Message 6>
message <Message 7>
message <Message 8>
message <Message 9>
```

Zabezpečte data správce sdílených front a soubory protokolu a soubory v systému Windows

Toto téma popisuje, jak můžete zabezpečit sdílené umístění pro data správce front a soubory žurnálu pomocí globální alternativní skupiny zabezpečení. Můžete sdílet umístění mezi různými instancemi správce front spuštěnými na různých serverech.

Obvykle nenastavíte sdílené umístění pro data správce front a soubory protokolu. Když instalujete produkt IBM MQ for Windows, instalační program vytvoří domovský adresář dle vašeho výběru pro všechny správce front, kteří jsou na tomto serveru vytvořeni. Zabezpečuje adresáře s lokální skupinou mqm a konfiguruje ID uživatele pro službu IBM MQ pro přístup k adresářům.

Když zabezpečujete sdílenou složku se skupinou zabezpečení, musí mít uživatel, který má oprávnění pro přístup ke složce, pověření skupiny. Předpokládejme, že složka na vzdáleném souborovém serveru je zabezpečena pomocí lokální skupiny mqm na serveru s názvem *mars*. Učinit uživatele, který spouští správce front, zpracovávat člena lokální skupiny mqm v systému *mars*. Uživatel má pověření, která odpovídají pověření složky na vzdáleném souborovém serveru. Pomocí těchto pověření je správce front schopen přistupovat k příslušným datům a protokoluje soubory ve složce. Uživatel, který spouští procesy správce front na jiném serveru, je členem jiné lokální skupiny produktu mqm, která nemá odpovídající pověření. Pokud správce front běží na jiném serveru než portál *mars*, nebude mít přístup k datům a souborům protokolu, které vytvořil, když běžel na serveru *mars*. I v případě, že uživatel domény uživatel domény, má jiná pověření, protože musí získat pověření z lokální skupiny mqm v systému *mars* a to nemůže provést z jiného serveru.

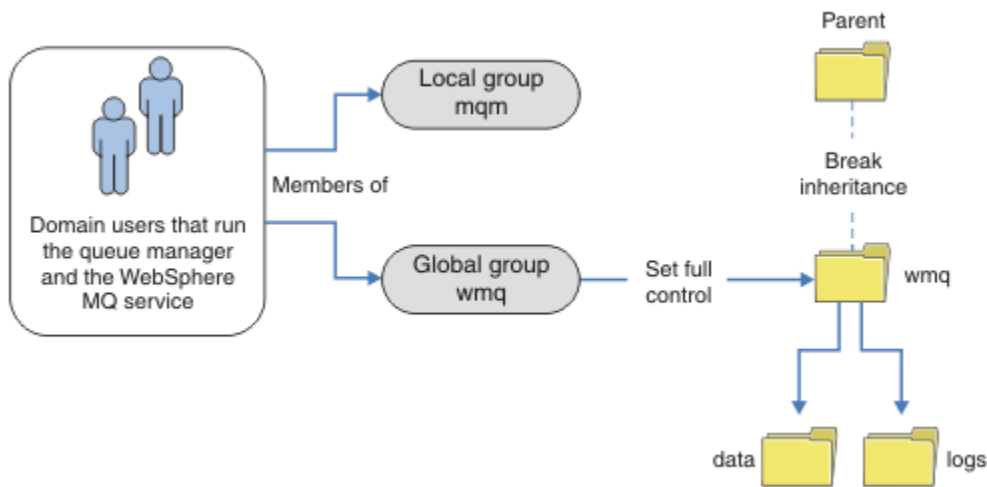
Zadání správce front s globální alternativní skupinou zabezpečení tento problém řeší; viz [Obrázek 75 na stránce 432](#). Zabezpečte vzdálenou složku s globální skupinou. Když jej vytvoříte v systému *mars*, předejte název globální skupiny ke správci front. Předejte název globální skupiny jako alternativní skupinu zabezpečení pomocí parametru `-a [r]` u příkazu `crtmqm`. Pokud přenesete správce front tak, aby byl spuštěn na jiném serveru, je název skupiny zabezpečení přenesen s tímto názvem. Název je přenesen ve stanici **AccessMode** v souboru `qm.ini` jako `SecurityGroup`. například:

```
AccessMode:
SecurityGroup=wmq\wmq
```

Stanza **AccessMode** v `qm.ini` obsahuje také `RemoveMQMAccess`; například:

```
AccessMode:
RemoveMQMAccess=<true\false>
```

Je-li tento atribut zadán s hodnotou `true` byla poskytnuta také skupina přístupů, lokální skupina mqm nemá udělen přístup k datovým souborům správce front.

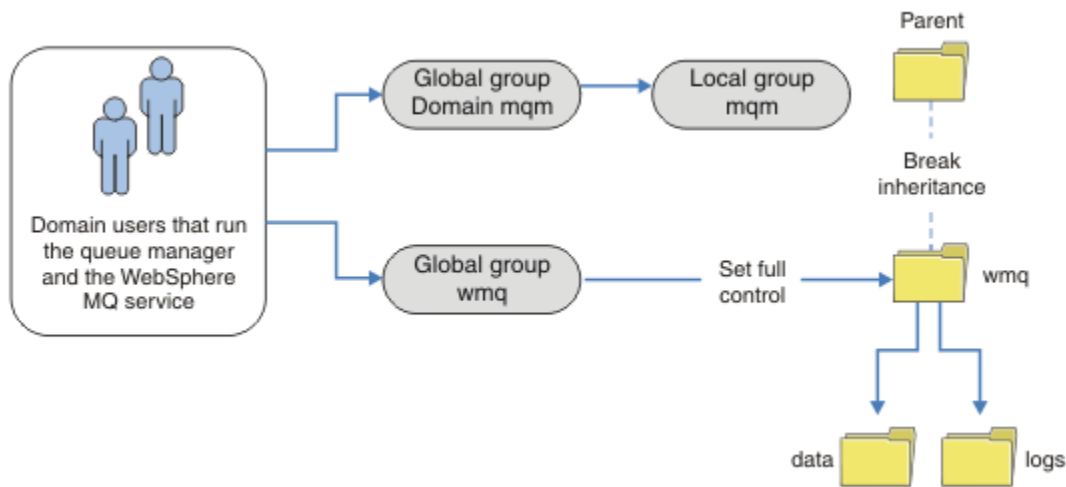


Obrázek 75. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (1)

Pro ID uživatele, kterým se mají spustit procesy správce front, mají-li mít odpovídající pověření globální skupiny zabezpečení, musí mít ID uživatele také globální rozsah. Nemůžete vytvořit lokální skupinu nebo činitele jako člena globální skupiny. V produktu [Obrázek 75 na stránce 432](#) se uživatelům, kteří spouštějí procesy správce front, zobrazují jako uživatelé domény.

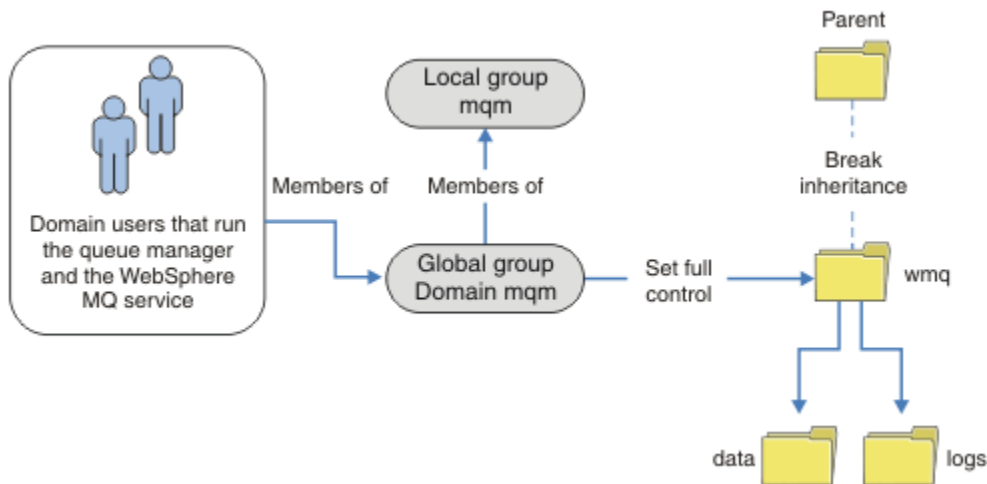
Pokud implementujete mnoho serverů IBM MQ, seskupení uživatelů v produktu [Obrázek 75 na stránce 432](#) není vhodné. Budete muset opakovat proces přidání uživatelů do lokálních skupin pro každý server IBM MQ. Namísto toho vytvořte na řadiči domény globální skupinu `Domain mqm` a vytvořte uživatele, kteří spouštějí členy IBM MQ skupiny `Domain mqm`, viz [Obrázek 76 na stránce 433](#). Když instalujete produkt IBM MQ jako instalaci domény, průvodce "Příprava produktu IBM MQ" automaticky vytvoří skupinu `Domain mqm` za člena lokální skupiny `mqm`. Tytéž uživatelé jsou v obou globálních skupinách `Domain mqm` a `wmq`.

Tip: Tytéž uživatelé mohou spouštět produkt IBM MQ na různých serverech, ale na individuálním serveru musíte mít různé uživatele ke spuštění produktu IBM MQ jako služby a mohou být spuštěny interaktivně. Pro každou instalaci na serveru musíte mít také různé uživatele. Zpravidla proto `Domain mqm` obsahuje mnoho uživatelů.



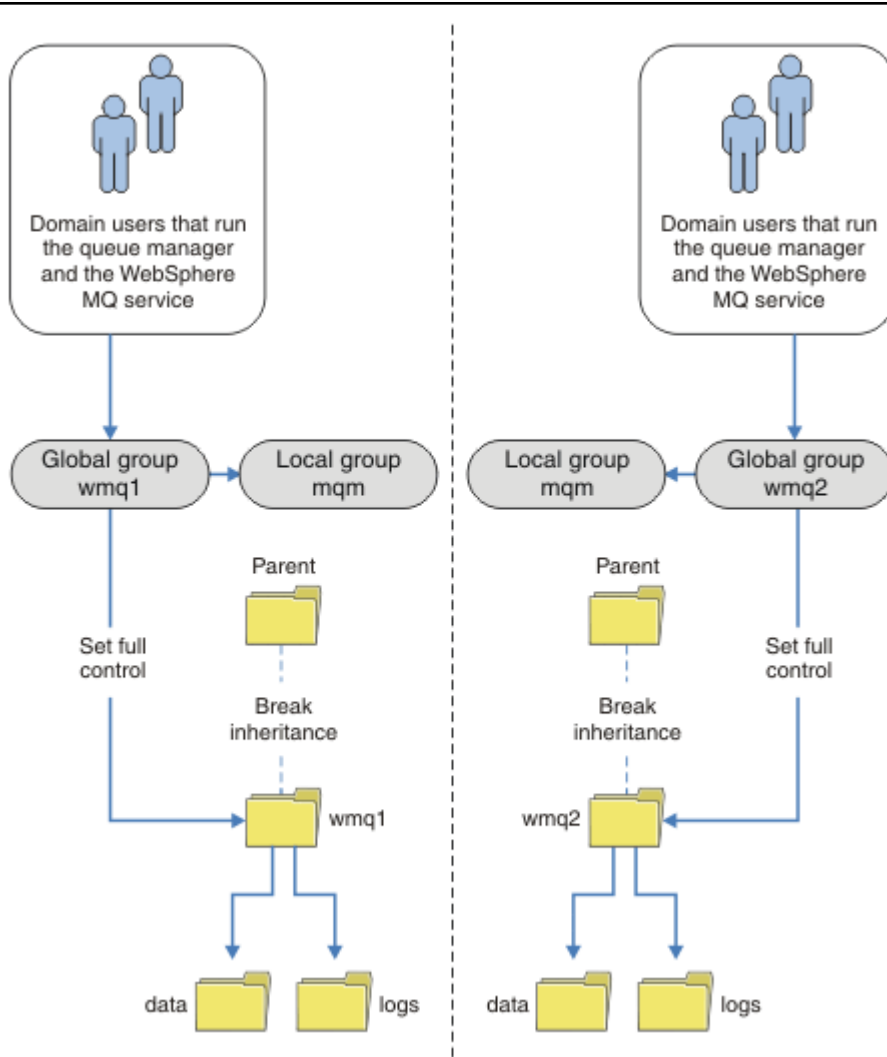
Obrázek 76. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (2)

Organizace v produktu Obrázek 76 na stránce 433 je zbytečně komplikovaná, jak stojí. Uspořádání má dvě globální skupiny se shodnými členy. Můžete zjednodušit organizaci a definovat pouze jednu globální skupinu; viz Obrázek 77 na stránce 433.



Obrázek 77. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (3)

Případně můžete potřebovat podrobnější úroveň řízení přístupu, kdy různí správci front omezení na přístup k různým složkám. Další informace viz Obrázek 78 na stránce 434. V produktu Obrázek 78 na stránce 434 jsou definovány dvě skupiny uživatelů domény v samostatných globálních skupinách za účelem zabezpečení různých protokolů správce front a datových souborů. Jsou zobrazeny dvě různé lokální skupiny mqm, které musí být na různých serverech IBM MQ. V tomto příkladu jsou správci front rozděleni do dvou sad s různými uživateli přidělenými na dvě sady. Tyto dvě sady mohou být testovacími a produkční správci front. Alternativní skupiny zabezpečení se nazývají wmq1 a wmq2. Musíte ručně přidat globální skupiny wmq1 a wmq2 do příslušných správců front podle toho, zda se nacházejí v testovacím nebo výrobním oddělení. Konfigurace nemůže využít výhod, které instalace produktu IBM MQ šíří Domain mqm do lokální skupiny mqm jako v Obrázek 77 na stránce 433, protože existují dvě skupiny uživatelů.



Obrázek 78. Zabezpečení dat správce front a protokolů pomocí alternativního činitele globálního zabezpečení (4)

Alternativním způsobem rozdělení dvou oddělení na logické oblasti by bylo jejich umístění ve dvou doménách systému Windows. V takovém případě se můžete vrátit k použití jednoduššího modelu zobrazeného v produktu [Obrázek 77](#) na stránce 433.

Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows

Toto téma popisuje, jak můžete zabezpečit alternativní umístění pro data správce front a soubory protokolu, a to jak pomocí lokální skupiny mqm, tak i pomocí alternativní skupiny zabezpečení.

Typicky nenastavíte alternativní umístění pro data správce front a soubory protokolu. Když instalujete produkt IBM MQ for Windows, instalační program vytvoří domovský adresář dle vašeho výběru pro všechny správce front, které jsou vytvořeny. Zabezpečuje adresáře s lokální skupinou mqm a konfiguruje ID uživatele pro službu IBM MQ pro přístup k adresářům.

Dva příklady demonstrují, jak nakonfigurovat řízení přístupu pro produkt IBM MQ. Příklady ukazují, jak vytvořit správce front se svými daty a protokoly v adresářích, které nejsou na datech a cestách protokolu vytvořených instalací. V prvním příkladu, “Čtení a zápis dat a souborů protokolu registrovaných lokální skupinou produktu mqm” na stránce 436, povolíte přístup k adresářům a adresářům protokolu tím, že udělíte oprávnění od lokální skupiny mqm. Druhý příklad, “Čtení a zápis dat a souborů protokolu, které jsou autorizovány alternativní lokální skupinou zabezpečení” na stránce 439, se liší v tom, že přístup k adresářům je autorizován alternativní skupinou zabezpečení. Když správce front přistupuje k adresářům pouze na jednom serveru, zabezpečení dat a souborů protokolu s alternativní skupinou zabezpečení

vám dává možnost zabezpečení různých správců front s různými lokálními skupinami nebo činiteli. Při přístupu k adresářům pomocí správce front spuštěného na různých serverech, jako je správce front s více instancemi, je jediným výběrem volby zabezpečení dat a souborů žurnálu s alternativní skupinou zabezpečení. Další informace naleznete v tématu [“Zabezpečte data správce sdílených front a soubory protokolu a soubory v systému Windows”](#) na stránce 431.

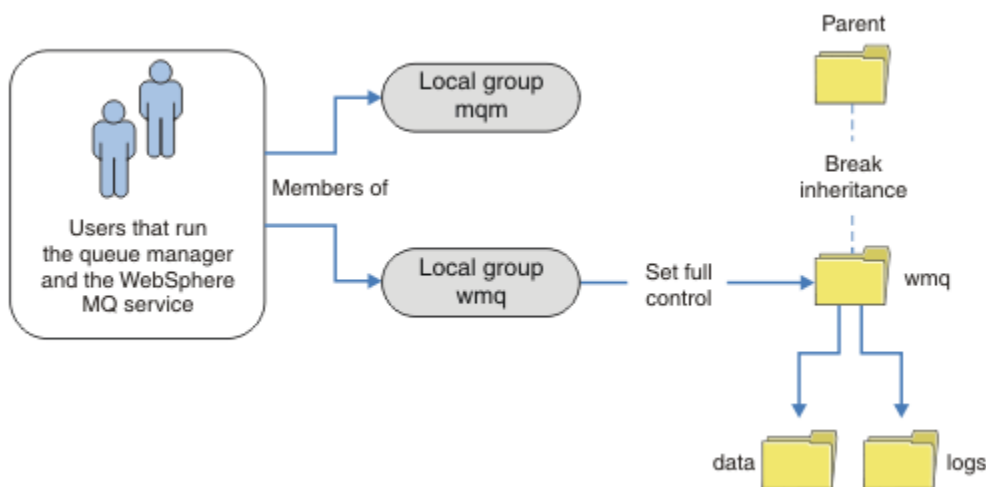
Konfigurace oprávnění zabezpečení dat správce front a souborů protokolu není běžná úloha v produktu Windows. Když instalujete produkt IBM MQ for Windows, buď zadejte adresáře pro data a protokoly správce front, nebo přijměte výchozí adresáře. Instalační program automaticky zabezpečuje tyto adresáře s lokální skupinou mqm a poskytuje jí úplné oprávnění k řízení. Proces instalace zajišťuje, že ID uživatele, který spouští správce front, je členem lokální skupiny mqm . Ostatní přístupová oprávnění k adresářům můžete upravit tak, aby odpovídala vašim požadavkům na přístup.

Přesunete-li data a adresář souborů protokolu do nových umístění, musíte nakonfigurovat zabezpečení nových umístění. Umístění těchto adresářů můžete změnit, pokud zálohujete správce front a obnovíte jej na jiný počítač nebo pokud změníte správce front tak, aby byl správcem front s více instancemi. Máte možnost výběru dvou způsobů, jak zabezpečit data správce front a adresáře protokolů ve svém novém umístění. Adresáře můžete zabezpečit omezením přístupu k lokální skupině mqm , nebo můžete omezit přístup k libovolné skupině zabezpečení dle vašeho výběru.

Potrvá nejméně několik kroků k zabezpečení adresářů pomocí lokální skupiny produktu mqm . Nastavte oprávnění k datům a adresářům protokolu tak, aby umožňovala plnou kontrolu celé skupiny produktu mqm . Typickým přístupem je kopírovat existující sadu oprávnění a odebrat dědičnost z nadřizené položky. Oprávnění jiných činitelů pak můžete odebrat nebo omezit.

Spustíte-li správce front pod jiným ID uživatele do služby vytvořené pomocí průvodce přípravou produktu IBM MQ , musí být toto ID uživatele členem lokální skupiny mqm . Úloha [“Čtení a zápis dat a souborů protokolu registrovaných lokální skupinou produktu mqm”](#) na stránce 436 vás provede jednotlivými kroky.

Data správce front a soubory protokolu můžete také zabezpečit pomocí alternativní skupiny zabezpečení. Proces zabezpečení dat správce front a souborů žurnálu s alternativní skupinou zabezpečení má řadu kroků, které odkazují na produkt [Obrázek 79](#) na stránce 435. Jako příklad alternativní skupiny zabezpečení je použita lokální skupina wmq.



Obrázek 79. Zabezpečení dat správce front a protokolů pomocí alternativní lokální skupiny zabezpečení, wmq

1. Buď vytvořte samostatné adresáře pro data a protokoly správce front, společný adresář nebo společný nadřizovaný adresář.
2. Zkopírujte existující sadu zděděných oprávnění pro adresáře nebo nadřizovaný adresář a upravte je podle svých potřeb.

3. Zabezpečte adresáře, které mají obsahovat správce front a protokoly, a to tak, že dáte alternativní skupině, `wmq`, plnou kontrolu oprávnění k adresářům.
4. Udělit oprávnění všech ID uživatelů, která spouštějí správce front, zpracuje pověření alternativní skupiny zabezpečení nebo činitele:
 - a. Definujete-li uživatele jako alternativního činitele zabezpečení, musí být uživatel stejného uživatele, pod kterým bude spuštěn správce front. Uživatel musí být členem lokální skupiny `mqm`.
 - b. Definujete-li lokální skupinu jako alternativní skupinu zabezpečení, přidejte uživatele, pod kterým bude správce front spuštěn, do alternativní skupiny. Uživatel musí být také členem lokální skupiny `mqm`.
 - c. Definujete-li globální skupinu jako alternativní skupinu zabezpečení, viz [“Zabezpečte data správce sdílených front a soubory protokolu a soubory v systému Windows”](#) na stránce 431.
5. Vytvořte správce front s uvedením alternativní skupiny zabezpečení nebo činitele v příkazu `crtmqm` s parametrem `-a`.

Čtení a zápis dat a souborů protokolu registrovaných lokální skupinou produktu mqm

Tato úloha popisuje, jak vytvořit správce front s daty a soubory protokolů uložené v libovolném adresáři dle vašeho výběru. Přístup k souborům je zabezpečen lokální skupinou `mqm`. Adresář není sdílený.

Než začnete

1. Nainstalujte produkt IBM MQ for Windows jako primární instalaci.
2. Spusťte průvodce "Příprava produktu IBM MQ". Pro tuto úlohu nakonfigurujte instalaci tak, aby se spouštěla s ID lokálního uživatele, nebo ID uživatele domény. Nakonec, chcete-li dokončit všechny úlohy v produktu [“Windows domén a správců front s více instancemi”](#) na stránce 405, musí být tato instalace nakonfigurována pro doménu.
3. Přihlaste se s oprávněním administrátora, abyste mohli provést první část úlohy.

Informace o této úloze

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolů uložených v adresáři dle vaší volby. Jsou připojeny k úloze, [“Windows domén a správců front s více instancemi”](#) na stránce 405.

V systému Windows můžete vytvořit výchozí data a cesty k protokolu pro produkt IBM MQ for Windows v libovolném adresáři dle vašeho výběru. Průvodce instalací a konfigurací automaticky poskytuje lokální skupinu `mqm` a ID uživatele, který spouští procesy správce front, přístup k adresářům. Pokud vytvoříte správce front, který uvádí různé adresáře pro data správce front a soubory protokolu, musíte nakonfigurovat úplné oprávnění pro řízení k adresářům.

V tomto příkladu dáte správci front plnou kontrolu nad svými daty a soubory protokolu tím, že dáte lokálnímu oprávnění skupiny `mqm` oprávnění k adresáři `c:\wmq`.

Příkaz `crtmqm` vytvoří správce front, který se spustí automaticky, když se pracovní stanice spustí pomocí služby IBM MQ.

Úloha je názorná; používá specifické hodnoty, které můžete změnit. Hodnoty, které můžete změnit, jsou kurzívou. Na konci úlohy postupujte podle pokynů a odeberte všechny provedené změny.

Postup

1. Otevřete příkazový řádek.
2. Zadejte příkaz:

```
md c:\wmq\data, c:\wmq\logs
```

3. Nastavte oprávnění k adresářům tak, aby povolovala lokální skupině `mqm` přístup pro čtení a zápis.

```
cacls c:\wmq/T /E /G mqm:F
```

Odezva systému:

```
processed dir: c:\wmq
processed dir: c:\wmq\data
processed dir: c:\wmq\logs
```

4. Volitelné: Přepněte na ID uživatele, které je členem lokální skupiny mqm .

Můžete pokračovat jako administrátor, ale v případě realistické provozní konfigurace pokračovat s ID uživatele s více omezenými právy. ID uživatele musí být alespoň členem lokální skupiny mqm . Je-li instalace produktu IBM MQ konfigurována jako část domény, vytvořte ID uživatele jako člena skupiny Domain mqm . Průvodce "Příprava produktu IBM MQ " učiní globální skupinu Domain mqm členem lokální skupiny mqm , takže nemusíte vytvářet ID uživatele přímo členem lokální skupiny mqm .

5. Vytvořte správce front.

```
crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md c:\wmq\data -ld c:\wmq\logs QMGR
```

Odezva systému:

```
IBM MQ queue manager created.
Directory 'c:\wmq\data\QMGR' created.
The queue manager is associated with installation '1'
Creating or replacing default objects for queue manager 'QMGR'
Default objects statistics : 74 created. 0 replaced.
Completing setup.
Setup completed.
```

6. Zkontrolujte, zda jsou adresáře vytvořené správcem front umístěny v adresáři c : \wmq .

```
dir c:\wmq/D /B /S
```

7. Zkontrolujte, zda mají soubory oprávnění ke čtení a zápisu, nebo úplné oprávnění pro lokální skupinu mqm .

```
cacls c:\wmq\*.*
```

Jak pokračovat dále

Otestujte správce front tak, že do fronty vložíte zprávu do fronty.

1. Spusťte správce front.

```
strmqm QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation '1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
```

Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.

2. Vytvořte testovací frontu.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

Odezva systému:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.  
Starting MQSC for queue manager QMGR.
```

```
1 : define qlocal(QTEST)  
AMQ8006: IBM MQ queue created.  
One MQSC command read.  
No commands have a syntax error.  
All valid MQSC commands were processed.
```

3. Vložte testovací zprávu pomocí ukázkového programu **amqspout**.

```
echo 'A test message' | amqspout QTEST QMGR
```

Odezva systému:

```
Sample AMQSPUT0 start  
target queue is QTEST  
Sample AMQSPUT0 end
```

4. Získejte testovací zprávu pomocí ukázkového programu **amqsget**.

```
amqsget QTEST QMGR
```

Odezva systému:

```
Sample AMQSGET0 start  
message <A test message>  
Wait 15 seconds ...  
no more messages  
Sample AMQSGET0 end
```

5. Zastavte správce front.

```
endmqm -i QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

IBM MQ queue manager 'QMGR' deleted.

7. Odstraňte adresáře, které jste vytvořili.

Tip: Přidejte do příkazů volbu /Q , abyste zabránili příkazu, aby se vymazal každý soubor nebo adresář.

```
del /F /S C:\wmq\*. *  
rmdir /S C:\wmq
```

Související pojmy

[“Windows domén a správců front s více instancemi” na stránce 405](#)

Správce front s více instancemi v produktu Windows vyžaduje, aby byla sdílena data a protokoly. Sdílení musí být přístupné pro všechny instance správce front spuštěných na různých serverech nebo pracovních stanicích. Konfigurujte správce front a sdílejte jej jako součást domény produktu Windows . Správce front může být spuštěn na pracovní stanici nebo na serveru domén nebo na řadiči domény.

Související úlohy

[Čtení a zápis dat a souborů protokolu, které jsou autorizovány alternativní lokální skupinou zabezpečení](#)
Tato úloha ukazuje, jak použít parametr -a u příkazu **crtmqm** . Příznak poskytuje správci front alternativní lokální skupinu zabezpečení, aby jí udělil přístup k jeho protokolových a datových souborech.

[“Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 418](#)

[“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény” na stránce 406](#)

Čtení a zápis dat a souborů protokolu, které jsou autorizovány alternativní lokální skupinou zabezpečení
Tato úloha ukazuje, jak použít parametr -a u příkazu **crtmqm** . Příznak poskytuje správci front alternativní lokální skupinu zabezpečení, aby jí udělil přístup k jeho protokolových a datových souborech.

Než začnete

1. Nainstalujte produkt IBM MQ for Windows jako primární instalaci.
2. Spusťte průvodce "Příprava produktu IBM MQ " . Pro tuto úlohu nakonfigurujte instalaci tak, aby se spouštěla s ID lokálního uživatele, nebo ID uživatele domény. Nakonec, chcete-li dokončit všechny úlohy v produktu [“Windows domén a správců front s více instancemi” na stránce 405](#), musí být tato instalace nakonfigurována pro doménu.
3. Přihlaste se s oprávněním administrátora, abyste mohli provést první část úlohy.

Informace o této úloze

Tato úloha je jednou ze sady souvisejících úloh, které ilustrují přístup k datům správce front a protokolům souborů. Úlohy ukazují, jak vytvořit správce front s oprávněním ke čtení a zápisu dat a souborů protokolů uložených v adresáři dle vaší volby. Jsou připojeny k úloze, [“Windows domén a správců front s více instancemi” na stránce 405](#).

V systému Windows můžete vytvořit výchozí data a cesty k protokolu pro produkt IBM MQ for Windows v libovolném adresáři dle vašeho výběru. Průvodce instalací a konfigurací automaticky poskytuje lokální skupinu mqm a ID uživatele, který spouští procesy správce front, přístup k adresářům. Pokud vytvoříte správce front, který uvádí různé adresáře pro data správce front a soubory protokolu, musíte nakonfigurovat úplné oprávnění pro řízení k adresářům.

V tomto příkladu poskytnete správci front alternativní lokální skupinu zabezpečení, která má oprávnění k úplnému řízení pro adresáře. Alternativní skupina zabezpečení poskytuje správci front oprávnění ke správě souborů v adresáři. Primárním účelem alternativní skupiny zabezpečení je autorizace alternativní globální skupiny zabezpečení. Chcete-li nastavit správce front pro více instancí, použijte alternativní globální skupinu zabezpečení. V tomto příkladu nakonfigurujete lokální skupinu, aby se seznámila s použitím alternativní skupiny zabezpečení bez instalace produktu IBM MQ v doméně. Je neobvyklé nakonfigurovat lokální skupinu jako alternativní skupinu zabezpečení.

Příkaz **crtmqm** vytvoří správce front, který se spustí automaticky, když se pracovní stanice spustí pomocí služby IBM MQ .

Úloha je názorný; používá specifické hodnoty, které můžete změnit. Hodnoty, které můžete změnit, jsou kurzívou. Na konci úlohy postupujte podle pokynů a odeberte všechny provedené změny.

Postup

1. Nastavení alternativní skupiny zabezpečení.

Alternativní skupina zabezpečení je obvykle skupina domén. V tomto příkladu vytvoříte správce front, který používá lokální alternativní skupinu zabezpečení. S lokální alternativní skupinou zabezpečení můžete provést tuto úlohu s instalací produktu IBM MQ , která není součástí domény.

- a) Spuštěním příkazu **lusrmgr.msc** otevřete okno Lokální uživatelé a skupiny.
- b) Klepněte pravým tlačítkem myši na **Skupiny > Nová skupina ...**
- c) V poli **Název skupiny** zadejte *altmqm* a klepněte na **Vytvořit > Zavřít**.
- d) Identifikujte ID uživatele, který spouští službu IBM MQ .
 - i) Klepněte na nabídku **Start > Spustit ...**, napište `services.msc` a klepněte na **OK**.
 - ii) Klepněte na službu IBM MQ v seznamu služeb a klepněte na kartu Přihlášení.
 - iii) Zapamatujte si ID uživatele a zavřete průzkumník služeb.
- e) Přidejte ID uživatele, který spouští službu IBM MQ , do skupiny *altmqm* . Přidejte také ID uživatele, se kterým se přihlašujete, abyste vytvořili správce front, a spusťte jej interaktivně.

Windows kontroluje oprávnění správce front pro přístup k datům a protokolů protokolů tím, že kontroluje oprávnění ID uživatele, který spouští procesy správce front. ID uživatele musí být členem skupiny *altmqm* , která má oprávnění k adresářům, přímo nebo nepřímo prostřednictvím globální skupiny.

Pokud jste produkt IBM MQ nainstalovali jako součást domény a chcete-li provést úlohu v produktu “Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény” na stránce 406, jsou ID uživatelů domény vytvořena v produktu “Vytvoření Active Directory a domény DNS pro IBM MQ” na stránce 409 *wmquser1* a *wmquser2* .

Pokud jste správce front neinstalovali jako část domény, výchozí ID lokálního uživatele, který spouští službu IBM MQ , je `MUSR_MQADMIN`. Hodláte-li provádět úlohy bez oprávnění administrátora, vytvořte uživatele, který je členem lokální skupiny *mqm* .

Chcete-li přidat *wmquser1* a *wmquser2* do *altmqm* , proveďte následující kroky. Pokud se vaše konfigurace liší, nahradte názvy ID uživatelů a skupiny.

- i) V seznamu skupin klepněte pravým tlačítkem myši na **altmqm > Vlastnosti > Přidat ...**
- ii) V okně Výběr uživatelů, počítačů nebo skupin vyberte *wmquser1* ; *wmquser2* a klepněte na **Kontrolovat názvy**.
- iii) Zadejte jméno a heslo administrátora domény v okně Zabezpečení produktu Windows a poté klepněte na tlačítko **OK > OK > Použít > OK**.

2. Otevřete příkazový řádek.

3. Restartujte službu IBM MQ .

Musíte restartovat službu, aby ID uživatele, pod kterým je spuštěna, získá přidavná pověření zabezpečení, která jste pro něj nakonfigurovali.

Zadejte příkazy:

```
endmqsvc  
startmqsvc
```

Systémové odezvy:

5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.
The MQ service for installation 'Installation1' ended successfully.

A:

5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.
The MQ service for installation 'Installation1' started successfully.

4. Zadejte příkaz:

```
md c:\wmq\data, c:\wmq\logs
```

5. Nastavte oprávnění k adresářům tak, aby povoloval přístup pro čtení a zápis u lokálního uživatele *user*.

```
cacls c:\wmq/T /E /G altmqm:F
```

Odezva systému:

```
processed dir: c:\wmq  
processed dir: c:\wmq\data  
processed dir: c:\wmq\logs
```

6. Volitelné: Přepněte na ID uživatele, které je členem lokální skupiny *mqm*.

Můžete pokračovat jako administrátor, ale v případě realistické provozní konfigurace pokračovat s ID uživatele s více omezenými právy. ID uživatele musí být alespoň členem lokální skupiny *mqm*. Je-li instalace produktu IBM MQ konfigurována jako část domény, vytvořte ID uživatele jako člena skupiny *Domain mqm*. Průvodce "Příprava produktu IBM MQ" učiní globální skupinu *Domain mqm* členem lokální skupiny *mqm*, takže nemusíte vytvářet ID uživatele přímo členem lokální skupiny *mqm*.

7. Vytvořte správce front.

```
crtmqm -a altmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md c:\wmq\data -ld c:\wmq\logs QMGR
```

Odezva systému:

```
IBM MQ queue manager created.  
Directory 'c:\wmq1\data\QMGR' created.  
The queue manager is associated with installation '1'  
Creating or replacing default objects for queue manager 'QMGR'  
Default objects statistics : 74 created. 0 replaced.  
Completing setup.  
Setup completed.
```

8. Zkontrolujte, zda jsou adresáře vytvořené správcem front umístěny v adresáři *c:\wmq*.

```
dir c:\wmq/D /B /S
```

9. Zkontrolujte, zda mají soubory oprávnění ke čtení a zápisu, nebo úplné oprávnění pro lokální skupinu *mqm*.

```
cacls c:\wmq\*.*
```

Jak pokračovat dále

Otestujte správce front tak, že do fronty vložíte zprávu do fronty.

1. Spustíte správce front.

```
stirmqm QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.  
The queue manager is associated with installation '1'.  
5 log records accessed on queue manager 'QMGR' during the log  
replay phase.  
Log replay for queue manager 'QMGR' complete.  
Transaction manager state recovered for queue manager 'QMGR'.  
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

2. Vytvoříte testovací frontu.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

Odezva systému:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2023. ALL RIGHTS RESERVED.  
Starting MQSC for queue manager QMGR.
```

```
1 : define qlocal(QTEST)  
AMQ8006: IBM MQ queue created.  
One MQSC command read.  
No commands have a syntax error.  
All valid MQSC commands were processed.
```

3. Vložte testovací zprávu pomocí ukázkového programu **amqspout**.

```
echo 'A test message' | amqspout QTEST QMGR
```

Odezva systému:

```
Sample AMQSPUT0 start  
target queue is QTEST  
Sample AMQSPUT0 end
```

4. Získejte testovací zprávu pomocí ukázkového programu **amqsget**.

```
amqsget QTEST QMGR
```

Odezva systému:

```
Sample AMQSGET0 start  
message <A test message>  
Wait 15 seconds ...  
no more messages  
Sample AMQSGET0 end
```

5. Zastavte správce front.

```
endmqm -i QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' ending.  
IBM MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

Tip: Přidejte do příkazů volbu /Q , abyste zabránili příkazu, aby se vymazal každý soubor nebo adresář.

```
del /F /S C:\wmq\*.*  
rmdir /S C:\wmq
```

Související úlohy

Čtení a zápis dat a souborů protokolu registrovaných lokální skupinou produktu mqm

Tato úloha popisuje, jak vytvořit správce front s daty a soubory protokolů uložené v libovolném adresáři dle vašeho výběru. Přístup k souborům je zabezpečen lokální skupinou mqm . Adresář není sdílený.

Vytvoření správce front s více instancemi v systému Linux

Příklad ukazuje, jak nastavit správce front s více instancemi na serveru Linux. Nastavení je malé pro ilustraci zúčastněných pojmů. Tento příklad je založen na systému Linux Red Hat Enterprise 5. Tyto kroky se liší od ostatních SYSTÉM UNIX.

Informace o této úloze

Příklad je nastaven na 2GHz notebooku se 3 GB RAM spuštěním Windows 7 Service Pack 1. Dva virtuální počítače VMware , Server1 a Server2, spustí Linux Red Hat Enterprise 5 ve snímcích 640 MB. Server Server1 je hostitelem síťového systému souborů (NFS), protokolů správce front a instance HA. Není obvyklé, aby se server NFS také hostili jedné z instancí správce front; to je zjednodušení příkladu. Server Server2 připojí protokoly správce front serveru Server1k instanci v pohotovostním režimu. Klient WebSphere MQ MQI se instaluje na další obraz 400 MB VMware , který spouští produkt Windows 7 Service Pack 1 a spouští ukázkové aplikace s vysokou dostupností. Všechny virtuální počítače jsou konfigurovány jako součást sítě hostitele VMware , a to z důvodů zabezpečení.

Poznámka: Měli byste umístit pouze data správce front na server NFS . Na systému NFS použijte k zajištění zabezpečení systému následující tři volby s příkazem mount:

noexec

Pomocí této volby zabráníte spuštění binárních souborů na systému NFS, což zabrání vzdálenému uživateli v spuštění nežádoucího kódu v systému.

nosuid

Pomocí této volby zabráníte použití bitů set-user-identifier a set-group-identifier, což zabrání vzdálenému uživateli získat vyšší oprávnění.

nodev

Pomocí této volby zastavíte používání nebo definování speciálních zařízení nebo blokových speciálních zařízení, která zabrání vzdálenému uživateli dostat se z vězení chroot.

Postup

1. Přihlaste se jako uživatel root.
2. Postupujte podle pokynů v tématu [Instalace produktu IBM MQ](#) k instalaci produktu IBM MQ, vytvoření uživatele a skupiny mqm a definování produktu /var/mqm.
3. Dokončete úlohu [Ověření chování sdíleného systému souborů](#) a zkontrolujte, zda systém souborů podporuje správce front s více instancemi.
4. Pro Server1 dokončete následující krok:
 - a. Vytvořte protokol a datové adresáře ve společné složce /MQHA, která má být sdílena. Příklad:
 - i) **mkdir** /MQHA
 - ii) **mkdir** /MQHA/logs
 - iii) **mkdir** /MQHA/qmgrs
5. Pro Server2 dokončete následující krok:
 - a. Vytvořte složku, /MQHA, chcete-li připojit sdílený systém souborů. Uchovat cestu stejně jako na serveru Server1. Příklad:
 - i) **mkdir** /MQHA
6. Ujistěte se, že adresáře MQHA jsou vlastněny uživatelem a skupinou mqm, a přístupová oprávnění jsou nastavena na rwx pro uživatele a skupinu. Například **ls -al** zobrazí drwxrwxr-x mqm mqm 4096 Nov 27 14:38 MQDATA .
 - a. **chown -R** mqm:mqm /MQHA
 - b. **chmod -R** ug+rwx /MQHA
7. Vytvořte správce front zadáním následujícího příkazu: **crtmqm -ld /MQHA/logs -md /MQHA/qmgrs QM1**
8. Přejist²/MQHA *(rw, sync, no_wdelay, fsid=0) na /etc/exports
9. Pro server Server1 proveďte následující kroky:
 - a. Spusťte démona NFS: **/etc/init.d/ nfs start**
 - b. Zkopírujte podrobnosti o konfiguraci správce front ze serveru Server1: .

```
dspmqlnf -o command QM1
```

a zkopírujte výsledek do schránky:

```
addmqinf -s QueueManager  
-v Name=QM1  
-v Directory=QM1  
-v Prefix=/var/mqm  
-v DataPath=/MQHA/qmgrs/QM1
```

10. Pro server Server2 proveďte následující kroky:
 - a. Připojte exportovaný systém souborů /MQHA zadáním následujícího příkazu: **mount -t nfs4 -o hard,intr Server1:/ /MQHA**
 - b. Vložte konfigurační příkaz správce front do serveru Server2:

```
addmqinf -s QueueManager  
-v Name=QM1  
-v Directory=QM1  
-v Prefix=/var/mqm  
-v DataPath=/MQHA/qmgrs/QM1
```

11. Spusťte instance správce front v jednom pořadí s parametrem -x: **strmqm -x QM1**.

² Volba '*' povoluje všechny počítače, které mohou dosáhnout tohoto připojení /MQHA pro čtení/zápis. Omezte přístup na produkční počítač.

Příkaz používaný ke spuštění instancí správce front musí být zadán ze stejné instalace produktu IBM MQ jako příkaz **addmqinf** . Chcete-li spustit a zastavit správce front z jiné instalace, je třeba nejprve nastavit instalaci přidruženou ke správci front pomocí příkazu **setmqm** . Další informace viz [setmqm](#).

Ověření správce front s více instancemi v systému Linux

Chcete-li ověřit konfiguraci správce front s více instancemi, použijte ukázkové programy **amqsghac**, **amqsphac** a **amqsmhac** . Toto téma poskytuje vzorovou konfiguraci pro ověření konfigurace správce front s více instancemi v systému Linux Red Hat Enterprise 5.

Ukázkové programy s vysokou dostupností používají automatické opětovné připojení klienta. Dojde-li k selhání připojeného správce front, klient se pokusí znovu připojit ke správci front ve stejné skupině správců front. Popis ukázek, [ukázkových programů vysoké dostupnosti](#), demonstruje opětovné připojení klienta pomocí správce front s jedinou instancí pro zjednodušení. Chcete-li ověřit konfiguraci správce front s více instancemi, můžete použít stejné ukázky s více správci front pro více instancí.

Příklad používá konfiguraci s více instancemi popsanou v části [“Vytvoření správce front s více instancemi v systému Linux”](#) na stránce 443. Použijte konfiguraci k ověření, že správce front s více instancemi se přepne na instanci v pohotovostním režimu. Zastavte správce front pomocí příkazu **endmqm** a použijte volbu **-s**, **switchover**, **option**. Programy klienta se znovu připojí k nové instanci správce front a budou pokračovat v práci s novou instancí po mírném zpoždění.

V tomto příkladu je klient spuštěn na systému Windows 7 Service Pack 1. Systém hostuje dva servery VMware Linux , na kterých běží správce front s více instancemi.

Ověření překonání selhání pomocí Průzkumníka IBM MQ

Než použijete ukázkové aplikace k ověření překonání selhání, spusťte na každém serveru Průzkumníka IBM MQ . Přidejte obě instance správce front do každého průzkumníku pomocí průvodce **Přidat vzdáleného správce front > Připojit přímo k víceinstanceinstanční správci front** . Ujistěte se, že obě instance jsou spuštěny, což umožňuje pohotovostní režim. Zavřete okno se spuštěnou instancí VMware s aktivní instancí, virtuálně vypněte server, nebo zastavte aktivní instanci, což umožňuje přepnutí do rezervní instance.

Poznámka: Pokud vypnete server, ujistěte se, že se nejedná o hostitelský systém /MQHA !

Poznámka: Volba **Povolit přepnutí na instanci v pohotovostním režimu** nemusí být k dispozici v dialogovém okně **Zastavit správce front** . Volba chybí, protože správce front je spuštěn jako správce front s jednou instancí. Musíte je spustit bez volby **Povolit instanci v pohotovostním režimu** . Pokud je váš požadavek na zastavení správce front odmítnut, podívejte se do okna **Podrobnosti** , je to možné, protože neexistuje žádná instance v pohotovostním režimu.

Ověření překonání selhání pomocí ukázkových programů

Vyberte server, na kterém má být spuštěna aktivní instance

Je možné, že jste zvolili jeden ze serverů pro hostování adresáře MQHA nebo systému souborů. Pokud plánujete otestovat překonání selhání zavřením okna VMware se spuštěným aktivním serverem, ujistěte se, že to není ten, který hostuje MQHA !

Na serveru, na kterém je spuštěna aktivní instance správce front

Poznámka: Spuštění kanálu produktu SVRCONN s parametrem MCAUSER nastaveným na hodnotu mqmje výhodné snížit počet kroků konfigurace uvedených v příkladu. Je-li zvoleno jiné ID uživatele a váš systém je nastaven jinak než ten, který se používá v příkladu, můžete se setkat s problémy s přístupovým oprávněním. Nepoužívejte mqm jako MCAUSER na vystaveném systému; je pravděpodobné, že se výrazně ohrozí bezpečnostní riziko.

1. Upravte hodnoty *ipaddr1* a *ipaddr2* a uložte následující příkazy v produktu /MQHA/*hasamples.tst* .

```
DEFINE QLOCAL(SOURCE) REPLACE
DEFINE QLOCAL(TARGET) REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(SVRCONN) TRPTYPE(TCP) +
MCAUSER('mqm') REPLACE
```

```

DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNAME(' ipaddr1 (1414), ipaddr2
(1414)') QMNAME(QM1) REPLACE
START CHANNEL(CHANNEL1)
DEFINE LISTENER(LISTENER.TCP) TRPTYPE(TCP) CONTROL(QMGR)
DISPLAY LISTENER(LISTENER.TCP) CONTROL
START LISTENER(LISTENER.TCP)
DISPLAY LSSTATUS(LISTENER.TCP) STATUS

```

2. Otevřete okno terminálu s cestou /MQHA a spusťte příkaz:

```
runmqsc -m QM1 < hasamples.tst
```

3. Ověřte, zda je modul listener spuštěný a má-li řízení správce front, a to buď kontrolou výstupu příkazu **runmqsc**.

```

LISTENER(LISTENER.TCP)CONTROL(QMGR)
LISTENER(LISTENER.TCP)STATUS(RUNNING)

```

Nebo pomocí Průzkumníka IBM MQ, že je spuštěn modul listener protokolu TCP/IP, a má Control = Queue Manager.

Na klientu

1. Zkopírujte tabulku připojení klienta AMQCLCHL.TAB z /MQHA/qmgrs/QM1.000/@ipcc na serveru na C:\ na klientovi.
2. Otevřete příkazový řádek s cestou C:\ a nastavte proměnnou prostředí MQCHLLIB tak, aby ukazovala na tabulku definic kanálů klienta (CCDT).

```
SET MQCHLLIB=C:\
```

3. Na příkazový řádek zadejte příkazy:

```

start amqsgnac TARGET QM1
start amqsmnac -s SOURCE -t TARGET -m QM1
start amqspnac SOURCE QM1

```

Na serveru, na kterém je spuštěna aktivní instance správce front

1. Proved'te jednu z následujících akcí:
 - Zavřete okno se spuštěnou instancí serveru VMware s obrazem aktivního serveru.
 - Pomocí Průzkumníka IBM MQ zastavte aktivní instanci správce front, což umožňuje přepnutí do instance v pohotovostním režimu a instruující se znovu připojitelné klienty k opětovnému připojení.
2. Tři klienti nakonec zjistí, že spojení je přerušeno, a pak se znovu připojí. V této konfiguraci, pokud zavřete okno serveru, trvá přibližně sedm minut, než se znovu ustanoví všechna tři připojení. Některá spojení se znovu ustanoví dobře před ostatními.

Výsledky

```
N:\>amqsphac SOURCE QM1
Sample AMQSPHAC start
target queue is SOURCE
message <Message 1>
message <Message 2>
message <Message 3>
message <Message 4>
message <Message 5>
17:05:25 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message <Message 6>
message <Message 7>
message <Message 8>
message <Message 9>
```

```
N:\>amqsmhac -s SOURCE -t TARGET -m QM1
Sample AMQSMHA0 start

17:05:25 : EVENT : Connection Reconnecting (Delay: 97ms)
17:05:48 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:53 : EVENT : Connection Reconnected
```

```
N:\>amqsgnac TARGET QM1
Sample AMQSGHAC start
message <Message 1>
message <Message 2>
message <Message 3>
message <Message 4>
message <Message 5>
17:05:25 : EVENT : Connection Reconnecting (Delay: 156ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message <Message 6>
message <Message 7>
message <Message 8>
message <Message 9>
```

Odstranění správce front s více instancemi

Chcete-li zcela odstranit správce front s více instancemi, je třeba pomocí příkazu **dltmqm** odstranit správce front a odebrat instance z jiných serverů pomocí příkazů **rmvmqinf** nebo **dltmqm**.

Spuštěním příkazu **dltmqm** odstraňte správce front s instancemi, které jsou definovány na jiných serverech, na libovolném serveru, na kterém je správce front definován. Není třeba spouštět příkaz **dltmqm** na stejném serveru, na kterém jste jej vytvořili. Poté spusťte příkaz **rmvmqinf** nebo **dltmqm** na všech ostatních serverech, které mají definici správce front.

Správce front můžete odstranit pouze v případě, že je zastaven. Ve chvíli, kdy jej odstraníte, nejsou spuštěny žádné instance a správce front striktně řečeno není ani jedním nebo více správcem front pro více instancí; je to jednoduše správce front, který má svá data správce front a protokoly na vzdáleném sdílení. Při odstranění správce front dojde k odstranění jeho dat a protokolů správce front a ze souboru `mqsc.ini` na serveru, na kterém jste zadali příkaz **dltmqm**, je odebrán oddíl správce front. Při odstraňování správce front je třeba mít přístup ke sdílenému síťovému sdílení, které obsahuje data správce front a protokoly.

Na jiných serverech, na kterých jste dříve vytvořili instance správce front, jsou na těchto serverech také položky v souborech `mqsc.ini`. Je třeba navštívit každý server a odstranit sekci správce front spuštěním příkazu **rmvmqinf** *název oddílu správce front*.

Pokud jste v systémech SYSTÉM UNIX a Linux umístili společný soubor `mqsc.ini` do síťového úložiště a odkazovali na něj ze všech serverů nastavením proměnné prostředí `AMQ_MQS_INI_LOCATION` na každém serveru, pak musíte správce front odstranit pouze z jednoho ze svých serverů, protože je k dispozici pouze jeden soubor `mqsc.ini`.

Příklad

První server

`dltmqm QM1`

Další servery, kde jsou definovány instance

`rmvmqinf QM1` nebo

`dltmqm QM1`

Spuštění a zastavení správce front s více instancemi

Spuštění a zastavení správce front konfigurovaného jako jedna instance nebo správce front s více instancemi.

Pokud jste definovali správce front s více instancemi na dvojici serverů, můžete správce front spustit na obou serverech buď jako správce front s jednou instancí, nebo jako správce front s více instancemi.

Chcete-li spustit správce front s více instancemi, spusťte správce front na jednom ze serverů s použitím příkazu **strmqm -x QM1**; volba `-x` povoluje instanci pro překonání selhání. Stane se *aktivní instancí*. Spusťte rezervní instanci na druhém serveru pomocí stejného příkazu **strmqm -x QM1**; volba `-x` povoluje, aby se instance spustila jako rezervní.

Správce front je nyní spuštěn s jednou aktivní instancí, která zpracovává všechny požadavky, a záložní instanci, která je připravena převzít, pokud dojde k selhání aktivní instance. Aktivní instance má udělen výlučný přístup k datům a protokolům správce front. Záložní server čeká na udělení výlučného přístupu k datům a protokolům správce front. Je-li do rezervní databáze udělen výlučný přístup, stane se aktivní instancí.

Můžete také ručně přepnout řízení na rezervní instanci zadáním příkazu **endmqm -s** na aktivní instanci. Příkaz **endmqm -s** ukončí běh aktivní instance bez ukončení činnosti pohotovostního režimu. Zámek výlučného přístupu k datům a protokolům správce front je uvolněn a rezervní databáze převezme funkci.

Můžete také spustit a zastavit správce front, který je konfigurován s více instancemi na různých serverech, jako správce front s jednou instancí. Pokud správce front spustíte bez použití volby `-x` u příkazu **strmqm**, nebude možné spouštět instance správce front konfigurovaného v jiných počítačích jako instance v pohotovostním režimu. Pokusíte-li se spustit jinou instanci, obdržíte odezvu, že instance správce front není povolena ke spuštění jako rezervní databáze.

Zastavíte-li aktivní instanci správce front s více instancemi pomocí příkazu **endmqm** bez volby `-s`, budou aktivní i rezervní instance zastaveny. Pokud zastavíte instanci v pohotovostním režimu pomocí příkazu **endmqm** s volbou `-x`, zastaví se jako záložní a aktivní instance bude pokračovat v činnosti. Nemůžete vydat příkaz **endmqm** bez volby `-x` v pohotovostním režimu.

Ve stejnou dobu mohou být spuštěny pouze dvě instance správce front; jedna z nich je aktivní instance a druhá instance je rezervní instance. Pokud spustíte dvě instance současně, produkt IBM MQ nemá žádnou kontrolu nad tím, který instance se stane aktivní instancí; je určen síťovým systémem souborů. První instance, která má získat výhradní přístup k datům správce front, se stane aktivní instancí.

Poznámka: Před restartováním správce front, který selhal, je třeba odpojit vaše aplikace od této instance správce front. Pokud tomu tak není, nemusí se správce front restartovat správně.

Sdílený systém souborů

Správce front pro více instancí používá síťový systém souborů ke správě instancí správce front.

Správce front s více instancemi automatizuje překonání selhání pomocí kombinace zámků systému souborů a sdílených dat správce front a protokolů. Pouze jedna instance správce front může mít výlučný přístup k datům a protokolům sdíleného správce front. Když se získá přístup, stane se aktivní instancí. Druhá instance, která nemá úspěch při získávání výlučného přístupu, bude čekat jako záložní instance, dokud nebudou zpřístupněna data a data správce front.

Systém souborů připojený k síti je odpovědný za uvolnění zámků, které ukládá pro aktivní instanci správce front. Pokud aktivní instance selže nějakým způsobem, síťový systém souborů uvolní zámky, které zadržuje pro aktivní instanci. Jakmile je uvolněn výlučný zámek, čeká se záložní správce front, který čeká

na získání zámku. Pokud uspěje, stane se aktivním instancí a má výlučný přístup k datům a protokolům správce front v rámci sdíleného systému souborů. Poté se pokračuje ve spuštění.

Související téma [Plánování podpory systému souborů](#) popisuje, jak lze nastavit a zkontrolovat, zda váš systém souborů podporuje správce front s více instancemi.

Správce front s více instancemi vás neochrání před selháním v systému souborů. Existuje celá řada způsobů, jak chránit vaše data.

- Investujte do spolehlivého úložiště, jako je pole RAID (redundant disk array), a zahrňte je do síťového systému souborů, který má odolnost sítě.
- Zazálohujte lineární protokoly IBM MQ na alternativní média, a pokud se médium primárního protokolu nezdaří, proveďte obnovu pomocí protokolů na alternativním médiu. Ke správě tohoto procesu můžete použít správce front zálohování.

Více instancí správce front

Správce front s více instancemi je odolný, protože používá pohotovostní instanci správce front k obnovení dostupnosti správce front po selhání.

Replikace instancí správce front je velmi účinným způsobem pro zlepšení dostupnosti procesů správce front. Použití jednoduchého modelu dostupnosti, pouze pro ilustraci: je-li spolehlivost jedné instance správce front 99% (více než jeden rok, kumulativní výpadek je 3.65 dní), pak přidání další instance správce front zvýší dostupnost na 99.99% (více než jeden rok, kumulativní výpadek přibližně za hodinu).

Tento model je příliš jednoduchý na to, aby vám poskytl praktické numerické odhady dostupnosti. Chcete-li modelovat dostupnost realisticky, musíte sbírat statistiku pro střední dobu mezi poruchami (MTBF) a průměrnou dobu na opravu (MTTR) a pravděpodobnostní rozdělení času mezi poruchami a časy oprav.

Termín správce front s více instancemi odkazuje na kombinaci aktivních a rezervních instancí správce front, které sdílejí data a protokoly správce front. Správci front s více instancemi vás ochrání před selháním procesů správce front tím, že budou mít jednu instanci správce front aktivní na jednom serveru, a další instanci správce front v pohotovostním režimu na jiném serveru, která je připravena k převzetí automaticky, pokud dojde k selhání aktivní instance.

Přepnutí nebo přeprnutí

Instance správce front v pohotovostním režimu přebírá z aktivní instance buď na požadavek (přepnutí), nebo když dojde k selhání aktivní instance (přepnutí při selhání).

- *Přepnutí* se provede tehdy, když se instance rezervní databáze spustí jako odpověď na příkaz **endmqm -s**, který je vydán do aktivní instance správce front. Můžete určit parametry **endmqm -c**, **-i** nebo **-p**, které určují, jak je správce front náhle ukončen.

Poznámka: Přepnutí se provede pouze v případě, že je instance správce front v pohotovostním režimu již spuštěna. Příkaz **endmqm -s** uvolní zámek aktivního správce front a povolí přepnutí: nespustí instanci správce front v pohotovostním režimu.

- *Překonání selhání* nastane, když je zámek na datech správce front v držení aktivní instance uvolněn, protože se neočekávaně zastavil instance (tj. bez zadání příkazu **endmqm**).

Když se záložní instance převezme jako aktivní instance, zapíše zprávu do protokolu chyb správce front.

Reconnetable klienti jsou automaticky znovu připojeni, když selže správce front nebo se přepíná. Chcete-li požadovat opětovné připojení klienta, nemusíte do příkazu **endmqm** zahrnout příznak **-r**. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Pokud zjistíte, že nelze restartovat selhání instance, i když došlo k překonání selhání a záložní instance se stala aktivní, zkontrolujte, zda se aplikace připojené lokálně k instanci, která selhala, odpojily od nezdařené instance.

Lokálně připojené aplikace musí skončit nebo se odpojit od nezdařené instance správce front, aby se instance, která selhala, restartovala. Všechny lokálně připojené aplikace používající sdílené vazby (což je výchozí nastavení), které se drží připojení k nezdařeným instancím instance, aby se zabránilo restartování instance.

Pokud není možné ukončit lokálně připojené aplikace, nebo zajistit, aby se odpojily při selhání lokální instance správce front, zvažte použití izolovaných vazeb. Lokálně připojené aplikace používající izolované vazby nezabrání restartování lokální instance správce front, a to i v případě, že se neodpojí.

Připojení kanálu a klienta znovu

Připojení kanálu a klienta je nezbytnou součástí obnovení zpracování zpráv po aktivaci instance správce front v pohotovostním režimu.

Instance správce front s více instancemi jsou instalovány na serverech s různými síťovými adresami. Je třeba nakonfigurovat kanály a kanály produktu IBM MQ s informacemi o připojení pro všechny instance správce front. Když se záloha převezme, klienti a kanály jsou automaticky znovu připojeni k nově aktivní instanci správce front na nové síťové adrese. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Návrh se liší od způsobu práce s vysokou dostupností, jako jsou například práce typu HA-CMP. Objekt HA-CMP poskytuje virtuální adresu IP pro klastr a přenáší adresu k aktivnímu serveru. IBM MQ opětovné připojení nemění nebo přesměrovává adresy IP. Pracuje tak, že se znovu propojí s použitím síťových adres, které jste definovali v definicích kanálů a připojeních klientů. Jako administrátor musíte definovat síťové adresy v definicích kanálů a připojení klienta ke všem instancím libovolného správce front s více instancemi. Nejlepší způsob konfigurace síťových adres pro správce front s více instancemi závisí na připojení:

Kanály správce front

Atribut CONNAME kanálů je čárkami oddělený seznam názvů připojení; například `CONNAME('127.0.0.1(1234), 192.0.2.0(4321)')`. Připojení se zkoušejí v pořadí uvedeném v seznamu připojení, dokud nebude úspěšně ustanoveno připojení. Není-li připojení úspěšné, kanál se pokusí znovu připojit.

Kanály klastru

Obvykle není zapotřebí žádná další konfigurace pro vytvoření správců front s více instancemi v klastru.

Pokud se správce front připojí ke správci front úložiště, zjistí úložiště síťovou adresu správce front. Tento parametr odkazuje na CONNAME kanálu produktu CLUSRCVR na správci front. Při použití protokolu TCPIP správce front automaticky nastaví parametr CONNAME, pokud jej vynecháte, nebo jej konfiguruje na prázdné místo. Když se převezme rezervní instance, jeho adresa IP nahradí adresu IP předchozí aktivní instance jako CONNAME.

Je-li to nezbytné, můžete ručně nakonfigurovat CONNAME se seznamem síťových adres instancí správce front.

Připojení klienta

Připojení klienta mohou používat seznamy připojení nebo skupiny správců front k výběru alternativních připojení. Je třeba, aby klienti byli kompilováni ke spuštění s klientskými knihovnami klienta IBM WebSphere MQ 7.0.1 nebo lepší. Musí být připojeny alespoň ke správci front produktu Verze 7.0.1.

Když dojde k překonání selhání, opětovné připojení zabere nějaký čas. Záložní správce front musí dokončit spuštění. Klienti, kteří byli připojeni k selhání správce front, musí zjistit selhání připojení a spustit nové připojení klienta. Pokud nové připojení klienta vybere rezervní správce front, který se stal nově aktivním, je klient znovu připojen ke stejnému správci front.

Je-li klient v polovině volání MQI během opětovného připojení, musí před dokončením volání tolerovat delší čekání.

Pokud dojde k selhání během dávkového přenosu na kanálu zpráv, dávka se vrátí zpět a restartuje.

Přepnutí je rychlejší než přestavení a trvá pouze tak dlouho, jako je zastavování jedné instance správce front a spuštění druhé. Pro správce front s pouhými několika záznamy protokolu k přehrání může v nejlepším přepnutí trvat několik sekund. Chcete-li odhadnout, jak dlouho trvá překonání selhání, musíte přidat čas, který trvá, než bude detekováno selhání. Nejlepší detekce trvá 10 sekund a může to trvat několik minut, v závislosti na síti a systému souborů.

Obnova aplikace

Obnova aplikací je automatické pokračování zpracování aplikací po překonání selhání. Obnova aplikace po překonání selhání vyžaduje důkladný návrh. Některé aplikace vyžadují, aby došlo k překonání selhání.

Cílem obnovy aplikace je, aby aplikace pokračovala ve zpracování pouze s krátkou prodlevou. Než budete pokračovat v novém zpracování, aplikace se musí vrátit zpět a znovu odeslat pracovní jednotku, kterou zpracovával během selhání.

Problém při zotavení aplikace ztrácí kontext, který je sdílen mezi produktem IBM MQ MQI client a správcem front a který je uložen ve správci front. IBM MQ MQI client obnovuje většinu kontextu, ale existují některé části kontextu, které nelze spolehlivě obnovit. V následujících částech jsou popsány některé vlastnosti obnovy aplikací a informace o tom, jak ovlivňují zotavení aplikací připojených ke správci front s více instancemi.

Transakční systém zpráv

Z pohledu doručování zpráv nemění překonání selhání trvalé vlastnosti systému zpráv produktu IBM MQ . Pokud jsou zprávy trvalé a jsou správně spravovány v rámci jednotek práce, zprávy se během překonání selhání neztratí.

Z pohledu zpracování transakcí jsou transakce buď zálohovány nebo potvrzeny po překonání selhání.

Nepotvrzené transakce jsou odvolány. Po překonání selhání obdrží znovu připojitelná aplikace MQRC_BACKED_OUT kód příčiny, aby označoval, že transakce se nezdařila. Poté musí transakci znovu spustit znovu.

Potvrzené transakce jsou transakce, které dosáhly druhé fáze dvoufázového potvrzovacího procesu nebo transakce s jednou fází (pouze zprávy), které začaly MQCMIT.

Je-li správce front koordinátorem transakce a MQCMIT zahájil druhou fázi své dvoufázové operace commit před selháním, transakce se úspěšně dokončí. Dokončení je pod kontrolou správce front a bude pokračovat, když je správce front spuštěn znovu. V repřipojitelné aplikaci je volání MQCMIT normálně dokončeno.

V jednofázovém potvrzení, které zahrnuje pouze zprávy, je transakce, která zahájila zpracování potvrzení, za normálních okolností pod kontrolou správce front, jakmile je spuštěna znovu. V repřipojitelné aplikaci se MQCMIT dokončí normálně.

Znovu připojitelné klienti mohou používat transakce s jednoduchou fází pod kontrolou správce front jako koordinátor transakcí. Rozšířený transakční klient nepodporuje opětovné připojení. Je-li požadováno opětovné připojení, když se připojuje transakční klient, připojení bude úspěšné, ale bez možnosti opětovného připojení. Připojení se chová, jako by se nepřipojitelné k tabulce.

Restart aplikace nebo pokračování

Překonání selhání přeruší aplikaci. Po selhání se může aplikace restartovat od začátku, nebo může pokračovat ve zpracování po přerušení. Tento příkaz se nazývá *automatické opětovné připojení klienta*. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Pomocí aplikace IBM MQ MQI client můžete nastavit volbu připojení pro automatické opětovné připojení klienta. Volby jsou MQCNO_RECONNECT nebo MQCNO_RECONNECT_Q_MGR. Není-li nastavena žádná volba, klient se nepokusí znovu připojit automaticky a selhání správce front se vrátí klientovi MQRC_CONNECTION_BROKEN . Můžete navrhnout klienta, abyste se pokusili spustit nové připojení zadáním nového volání MQCONN nebo MQCONNX .

Programy serveru je třeba restartovat; správce front nemůže automaticky znovu připojit, a to v okamžiku, kdy došlo k selhání správce front nebo serveru. Programy serveru IBM MQ se při selhání instance správce front s více instancemi zpravidla nerestartuje na instanci správce front v pohotovostním režimu.

Program na serveru IBM MQ můžete automatizovat, aby se restartoval na záložním serveru dvěma způsoby:

1. Zabalte aplikaci serveru jako službu správce front. Restartuje se, když se správce front v pohotovostním režimu restartuje.
2. Zadejte vlastní logiku pro překonání selhání, která se spustí například při spuštění zprávy protokolu o překonání selhání, kterou zapsal záložní instance správce front. Instance aplikace pak musí po spuštění volat MQCONN nebo MQCONNX , aby bylo možné vytvořit připojení ke správci front.

Detekce překonání selhání

Některé aplikace si musí být vědomi překonání selhání, jiné nikoli. Zvažte tyto dva příklady.

1. Aplikace systému zpráv, která přijímá nebo přijímá zprávy prostřednictvím kanálu systému zpráv, standardně nevyžaduje spuštění správce front na druhém konci kanálu: pravděpodobně nebude ovlivněn, pokud správce front na druhém konci kanálu restartuje v rámci instance v pohotovostním režimu.
2. Aplikace IBM MQ MQI client zpracovává trvalý vstup zpráv z jedné fronty a ukládá trvalé odpovědi na zprávy do jiné fronty jako součást jediné transakce: pokud zpracovává kód příčiny MQRC_BACKED_OUT z MQPUT, MQGET nebo MQCMIT v rámci synchronizačního bodu restartováním pracovní jednotky, pak se žádné zprávy neztratí. Aplikace navíc nemusí provádět žádné speciální zpracování při pokusu o navázání spojení se selháním připojení.

Předpokládejme však, že v druhém příkladu je aplikace prohledáváním fronty a výběru zprávy ke zpracování pomocí volby MQGET , MQGMO_MSG_UNDER_CURSOR. Reconnction resetuje kurzor procházení a volání MQGET nevrátí správnou zprávu. V tomto příkladu se vyskytla aplikace, která má být informovaná o překonání selhání. Kromě toho musí před vydáním jiného příkazu MQGET pro zprávu pod kurzorem aplikace obnovit kurzor procházení.

Ztráta kurzoru při procházení představuje jeden příklad, jak se mění kontext aplikace po opětovném připojení. Další případy jsou dokumentovány v příručce [“Zotavení automaticky znovu připojeného klienta”](#) na stránce 453.

Máte tři alternativní vzory návrhu pro aplikace produktu IBM MQ MQI client po překonání selhání. Pouze jeden z nich není třeba detekovat překonání selhání.

Bez opětovného připojení

V tomto vzorku zastaví aplikace veškeré zpracování aktuálního připojení, jakmile dojde k přerušení spojení. Má-li aplikace pokračovat ve zpracování, musí vytvořit nové připojení ke správci front. Aplikace je zcela odpovědná za přenos všech informací o stavu, které vyžaduje, aby pokračovalo zpracování na novém připojení. Existující klientské aplikace, které se znovu připojí ke správci front po ztrátě spojení, jsou tímto způsobem zapsány.

Klient obdrží kód příčiny, například MQRC_CONNECTION_BROKEN nebo MQRC_Q_MGR_NOT_AVAILABLE , z dalšího volání MQI po ztrátě spojení. Aplikace musí vyřadit všechny své informace o stavu IBM MQ , jako jsou popisovače fronty, a vydat nové volání MQCONN nebo MQCONNX k vytvoření nového připojení a poté znovu otevřít objekty produktu IBM MQ , které potřebuje ke zpracování.

Výchozí chování MQI je pro popisovač připojení ke správci front, který má být nepoužitelný po ztrátě připojení ke správci front. Předvolba je ekvivalentní nastavení volby MQCNO_RECONNECT_DISABLED v systému MQCONNX , aby se zabránilo opětovnému připojení aplikace po překonání selhání.

Překonání selhání

Zapište aplikaci tak, aby nebyla ovlivněna překonáním selhání. Někdy je třeba pečlivě sledovat ošetřování chyb při řešení překonání selhání.

Reconnction aware

Zaregistrujte obslužnou rutinu událostí MQCBT_EVENT_HANDLER se správcem front. Obslužná rutina událostí se uveřejní v produktu MQRC_RECONNECTING , když se klient spustí při pokusu o opětovné připojení k serveru a MQRC_RECONNECTED po úspěšném opětovném připojení. Poté můžete spustit

rutinu tak, aby znovu vytvořila předvídatelný stav, takže klientská aplikace bude schopna pokračovat ve zpracování.

Zotavení automaticky znovu připojeného klienta

Překonání selhání je neočekávaná událost a pro automaticky připojovaného klienta k práci, jak je navrženo důsledky opětovného připojení, musí být předvídatelné.

Hlavním prvkem obratu neočekávaného selhání v předvídatelném a spolehlivém zotavení je použití transakcí.

V předchozí sekci byl zadán příklad “2” na stránce 452, který byl zadán IBM MQ MQI client pomocí lokální transakce pro koordinaci MQGET a MQPUT. Klient vydá chybu MQCMIT nebo MQBACK v odezvě na chybu MQRC_BACKED_OUT a poté znovu odešle zálohovanou transakci. Selhání správce front způsobí, že transakce bude vrácena a chování aplikace klienta zajistí, že nebudou ztraceny žádné transakce a žádné zprávy.

Ne všechny programové stavy jsou spravovány jako součást transakce, a proto je obtížné porozumět následkům opětovného připojení. Musíte vědět, jak opětovné připojení změní stav IBM MQ MQI client, aby bylo možné navrhnout aplikaci klienta, aby přežila překonání selhání správce front.

Můžete se rozhodnout navrhnout svou aplikaci bez speciálního kódu pro překonání selhání a s jinými chybami znovu zacházet s chybami opětovného připojení se stejnou logikou. Případně můžete zvolit, že opětovné připojení vyžaduje speciální zpracování chyb, a zaregistrujte obslužnou rutinu událostí s produktem IBM MQ ke spuštění rutiny pro překonání selhání. Rutina může pracovat se zpracováním opětovného připojení nebo nastavit příznak tak, aby indikoval vláknu hlavního programu, že když bude pokračovat ve zpracování, je třeba provést zpracování zotavení.

Prostředí IBM MQ MQI client si je vědomo samotné překonání selhání a obnovuje se tak, jak může, po opětovném připojení, uložením některých informací o stavu v klientovi a vydáním dalších volání MQI v zastoupení klientské aplikace za účelem obnovení stavu IBM MQ. Například jsou obnoveny objekty, které byly otevřené v bodu selhání, a dočasné dynamické fronty se otvírají se stejným názvem. Existují však změny, které jsou nevyhnutelné a vy potřebujete váš návrh na vypořádání se s těmito změnami. Změny lze rozdělit do pěti druhů:

1. Nová nebo dříve nediagnostikovaná chyba se vrací z volání MQI, dokud aplikační program neobnoví konzistentní nový stav kontextu.

Příklad přijetí nové chyby je návratový kód MQRC_CONTEXT_NOT_AVAILABLE při pokusu o předání kontextu po uložení kontextu před opětovným připojením. Kontext nelze obnovit po novém připojení, protože kontext zabezpečení nebyl předán neautorizovanému programu klienta. Chcete-li tak učinit, aby mohl škodlivý aplikační program získat kontext zabezpečení.

Obvykle aplikace zpracovávají běžné a předvídatelné chyby v pečlivě navrženém způsobem a relegují méně časté chyby na generickou obslužnou rutinu chyb. Obslužná rutina chyb se může odpojit od IBM MQ a znovu se znovu připojit, nebo dokonce zastavit program úplně. Chcete-li zlepšit kontinuitu, je možné, že se budete muset vypořádat s některými chybami jinak.

2. Netrvalé zprávy mohou být ztraceny.
3. Transakce jsou odvolány.
4. Volání MQGET nebo MQPUT použitá mimo bod synchronizace mohou být přerušeny s možnou ztrátou zprávy.
5. Při dlouhodobém čekání na volání MQI došlo k chybám způsobeným načasným načasným načasným čekáním.

Některé podrobnosti o ztrátě kontextu jsou uvedeny v následující sekci.

- Netrvalé zprávy jsou vyřazeny, pokud nebyly vloženy do fronty s volbou NPMCLASS (HIGH) a selhání správce front nepřeruší volbu ukládání přechodných zpráv při ukončení práce systému.
- Netrvalý odběr je ztracen, je-li přerušeno připojení. Při opětovném připojení se znovu zavádí. Zvažte použití trvalého odběru.

- Interval get-wait se přepočítá; pokud je překročen jeho limit, vrátí hodnotu MQRC_NO_MSG_AVAILABLE. Podobně se znovu vypočítá vypršení platnosti odběru tak, aby poskytly stejnou celkovou dobu vypršení platnosti.
- Pozice kurzoru pro procházení ve frontě je ztracena; je obvykle znovu vytvořena před první zprávou.
 - Volání MQGET , která uvádí MQGMO_BROWS_MSG_UNDER_CURSOR nebo MQGMO_MSG_UNDER_CURSOR, se nezdaří s kódem příčiny MQRC_NO_MSG_AVAILABLE.
 - Zprávy zamknuté pro procházení jsou odemčeny.
 - Procházet označené zprávy s rozsahem platnosti popisovače jsou neoznačené a lze je znovu procházet.
 - Ve většině případů jsou označené zprávy ve většině případů neoznačené.
- Kontext zabezpečení je ztracen. Pokusy o použití kontextu uložené zprávy, jako např. vložení zprávy s MQPMO_PASS_ALL_CONTEXT , selžou s produktem MQRC_CONTEXT_NOT_AVAILABLE.
- Tokeny zpráv jsou ztraceny. MQGET používající token zprávy vrátí kód příčiny MQRC_NO_MSG_AVAILABLE.

Poznámka: *MsgId* a *CorrelId*, protože jsou součástí zprávy, jsou zachovány se zprávou během překonání selhání, a proto MQGET pomocí *MsgId* nebo *CorrelId* pracuje podle očekávání.

- Zprávy vkládané do fronty pod bodem synchronizace v nepotvrzené transakci již nejsou k dispozici.
- Zpracování zpráv v logickém pořadí, nebo ve skupině zpráv, má za následek návratový kód MQRC_RECONNECT_INCOMPATIBLE po opětovném připojení.
- Volání MQI může vrátit MQRC_RECONNECT_FAILED spíše než obecnější MQRC_CONNECTION_BROKEN , které klienti obvykle přijímají dnes.
- Opětovné připojení během volání MQPUT mimo synchronizační bod vrátí hodnotu MQRC_CALL_INTERRUPTED , pokud IBM MQ MQI client neví, zda byla zpráva úspěšně doručena správci front. Opětovné připojení během MQCMIT se chová podobně.
- Příkaz MQRC_CALL_INTERRUPTED je vrácen-po úspěšném opětovném připojení-pokud produkt IBM MQ MQI client neobdržel od správce front žádnou odpověď, aby označil úspěch nebo selhání
 - Doručování trvalé zprávy pomocí volání MQPUT mimo synchronizační bod.
 - Doručování trvalé zprávy nebo zprávy s výchozí perzistencí pomocí volání MQPUT1 mimo synchronizační bod.
 - potvrzení transakce pomocí volání MQCMIT. Odezva se vrátí pouze po úspěšném opětovném připojení.
- Kanály jsou restartovány jako nové instance (mohou se také jednat o různé kanály), a proto se nezachová žádný stav ukončení kanálu.
- Dočasné dynamické fronty se obnoví jako část procesu obnovy klientů s možností opětovného připojení, které měly otevřené dočasné dynamické fronty. Žádné zprávy v dočasné dynamické frontě nejsou obnoveny, ale aplikace, které měly frontu otevřenou, nebo si zapamatovali název fronty, jsou schopny pokračovat ve zpracování.

Je zde možnost, že pokud je fronta používána jinou aplikací, než je ta, která ji vytvořila, nemusí být obnovena dostatečně rychle, aby mohla být přítomna, když se na ni bude příště odkazovat. Pokud například klient vytvoří dočasnou dynamickou frontu jako frontu pro odpovědi na frontu a do fronty bude vložena zpráva s odezvou, nemusí být fronta vrácena včas. V tomto případě by kanál obvykle umístil odpověď-na zprávu do fronty nedoručených zpráv.

Pokud aplikace klienta s možností opětovného připojení otevře dočasnou dynamickou frontu podle názvu (protože ji již vytvořila jiná aplikace) a poté dojde k opětovnému připojení, produkt IBM MQ MQI client nemůže znovu vytvořit dočasnou dynamickou frontu, protože ji nemá model k vytvoření. V rozhraní MQI může dočasnou dynamickou frontu v rámci modelu otevřít pouze jedna aplikace. Ostatní aplikace, které chtějí použít dočasnou dynamickou frontu, musí používat vazby MQPUT1 nebo vazby serveru nebo mohou znovu zkusit opětovné připojení, pokud se nezdaří.

Do dočasné dynamické fronty mohou být vloženy pouze přechodné zprávy a tyto zprávy se ztratí během překonání selhání. Tato ztráta má hodnotu true pro zprávy, které jsou do dočasné dynamické fronty

vloženy pomocí příkazu MQPUT1 během opětovného připojení. Pokud dojde k překonání selhání během operace MQPUT1, nemusí být zpráva vložena, ačkoli je parametr MQPUT1 úspěšný. Alternativním řešením tohoto problému je použití trvalých dynamických front. Každá aplikace pro vázání serveru může otevřít dočasnou dynamickou frontu podle názvu, protože ji nelze znovu připojit.

Zotavení dat a vysoká dostupnost

Řešení vysoké dostupnosti s pomocí správců front s více instancemi musí zahrnovat mechanismus k obnovení dat po selhání úložiště.

Správce front s více instancemi zvyšuje dostupnost procesů správce front, nikoli však dostupnost jiných komponent, jako je například systém souborů, který správce front používá k ukládání zpráv a další informace.

Jedním ze způsobů, jak zajistit vysokou dostupnost dat, je použití odolného datového úložiště odolných vůči síti. Můžete buď sestavit své vlastní řešení pomocí síťového systému souborů a odolného datového úložiště, nebo si můžete zakoupit integrované řešení. Chcete-li skloubit odolnost vůči zotavení z havárie, pak je k dispozici asynchronní replikace disku, která umožňuje replikaci disku přes desítky nebo stovky kilometrů.

Můžete nakonfigurovat způsob, jakým jsou mapovány různé adresáře produktu IBM MQ na paměťová média, abyste dosáhli co nejlepšího využití médií. Pro správce front *více instancí* je důležité rozlišovat mezi dvěma typy adresářů a souborů IBM MQ .

Adresáře, které musí být sdíleny mezi instancemi správce front.

Informace, které musí být sdíleny mezi různými instancemi správce front, se nacházejí ve dvou adresářích: z adresářů `qmgrs` a `logs` . Adresáře musí být na sdíleném síťovém systému souborů. Doporučuje se používat paměťová média, která poskytuje nepřetržitou vysokou dostupnost a vynikající výkon, protože data se neustále mění v podobě zpráv, které jsou vytvářeny a odstraňovány.

Adresáře a soubory, které nemají být sdíleny mezi instancemi správce front.

Některé jiné adresáře nemusí být sdíleny mezi různými instancemi správce front a jsou rychle obnoveny jiným způsobem než pomocí zrcadlového systému souborů.

- Spustitelné soubory IBM MQ a adresář nástrojů. Nahraďte opětovnou instalací nebo zálohováním a obnovením z archivu zálohovaného souboru.
- Informace o konfiguraci, které jsou upraveny pro instalaci jako celek. Informace o konfiguraci jsou spravovány produktem IBM MQ, jako je například soubor `mqsc.ini` v systémech Windows, SYSTÉM UNIX a Linux nebo část vlastní správy konfigurace, jako např. konfigurační skripty produktu **MQSC** . Zálohování a obnova pomocí archivu souborů.
- Výstup z instalace, jako jsou například trasování, protokoly chyb a soubory FFDC. Soubory se uloží do podadresářů `errors` a `trace` ve výchozím datovém adresáři. Výchozí datový adresář na systémech SYSTÉM UNIX a Linux je `/var/mqm`. V systému Windows je výchozím datovým adresářem instalační adresář produktu IBM MQ .

Správce front pro zálohování můžete také použít k provádění pravidelných záloh médií správce front s více instancemi pomocí lineárního protokolování. Záložní správce front neposkytuje obnovu, která je stejně rychlá jako ze zrcadleného systému souborů a neobnoví změny od poslední zálohy. Záložní mechanismus správce front je vhodnější pro použití ve scénářích zotavení z havárie v režimu offline, než je zotavení správce front po lokalizovaném selhání úložiště.

Kombinování řešení dostupnosti IBM MQ

Aplikace používají jiné funkce produktu IBM MQ ke zlepšení dostupnosti. Správci front s více instancemi doplňují jiné možnosti vysoké dostupnosti.

IBM MQ Klastry zvyšují dostupnost fronty

Můžete zvýšit dostupnost fronty vytvořením více definic fronty klastru; až do jedné z každé fronty v každém správci v klastru.

Předpokládejme, že člen klastru selže, a pak se odešle nová zpráva do fronty klastru. Pokud zpráva *nemá* pro přechod na správce front, který selhal, odešle se zpráva do jiného spuštěného správce front v klastru, který má definici fronty.

Ačkoli klastry výrazně zvyšují dostupnost, existují dva související scénáře selhání, které vedou ke zpoždění zpráv. Sestavení klastru pomocí správců front s více instancemi snižuje možnost opožděného zpoždění zprávy.

Manoované zprávy

Pokud se správce front v klastru nezdaří, žádné další zprávy, které mohou být směřovány do jiných správců front v klastru, jsou směřovány do správce front, který selhal. Zprávy, které již byly odeslány, jsou zakonovány, dokud se správce front, který selhal, znovu spustí.

Afinity

Afinita je termín používaný k popisu informací sdílených mezi dvěma jinak oddělenými výpočty. Existuje například afinita mezi aplikací odesílající zprávu požadavku na server a stejnou aplikací, která očekává zpracování odpovědi. Dalším příkladem může být posloupnost zpráv, zpracování každé zprávy v závislosti na předchozích zprávách.

Pokud odešlete zprávy do sdružených front, je třeba zvážit afinity. Potřebujete odeslat následné zprávy do stejného správce front, nebo může každá zpráva přejít na kteréhokoli člena klastru?

Pokud budete muset odesílat zprávy do stejného správce front v klastru a dojde k selhání, budou zprávy čekat v přenosové frontě odesílatele, dokud se správce front klastru, který selhal, znovu nespustí.

Je-li klastr konfigurován s víceinstanční správci front, bude zpoždění, které čeká na restartování správce front, restartováno, je omezeno na pořadí minut nebo na chvíli, kdy rezervní databáze převezme řízení. Když je rezervní databáze spuštěna, zahájí se zpracování zamalených zpráv, spustí se kanály do nově aktivované instance správce front a zprávy, které čekaly v přenosových frontách, začnou proudit.

Možným způsobem, jak nakonfigurovat klastr k odstranění zpráv zpožděných správcem front se selháním, je nasadit dva různé správce front na každý server v klastru a zajistit, aby jeden z nich byl aktivní a jeden jako záložní instance pro různé správce front. Jedná se o konfiguraci aktivní rezervní databáze a zvyšuje dostupnost klastru.

Kromě výhod snížené administrace a zvýšené rozšiřitelnosti mohou klastry poskytovat další prvky dostupnosti, které doplňují správce front s více instancemi. Klastry jsou chráněny proti jiným typům selhání, které ovlivňují jak aktivní, tak i rezervní instance správce front.

Nepřerušená služba

Klastr poskytuje nepřerušovanou službu. Nové zprávy přijaté klastrem se odešlou do aktivních správců front, které mají být zpracovány. Nespolehejte se na správce front s více instancemi, aby poskytoval nepřerušovanou službu, protože vyžaduje, aby správce front v pohotovostním režimu zjistil selhání a dokončil své spuštění, aby bylo možné kanály znovu připojit, a aby byly znovu odeslány selhané dávky zpráv.

Lokalizovaný výpadek

Existují praktická omezení pro to, jak daleko od sebe mohou být aktivní, záložní a servery systémů souborů, protože je třeba interaktivně pracovat s rychlostí milisekund, aby bylo možné dosáhnout přijatelného výkonu.

Klastrované správce front vyžadují zrychlení interakce v řádu mnoha sekund a mohou být geograficky rozptýleny kdekoli na světě.

Operační chyba

Použitím dvou různých mechanismů pro zvýšení dostupnosti snížíte pravděpodobnost, že provozní chyba, jako např. lidská chyba, bude ohrožovat vaše úsilí o dosažení dostupnosti.

Skupiny sdílení front zvyšují dostupnost zpracování zpráv

Skupiny sdílení front, které jsou k dispozici pouze v produktu z/OS, umožňují skupině správců front sdílet obsluhování fronty. Dojde-li k selhání jednoho správce front, budou ostatní správci front nadále zpracovávat všechny zprávy ve frontě. Správci front s více instancemi nejsou v produktu z/OS podporováni a doplňují skupiny sdílení front pouze jako součást širší architektury systému zpráv.

IBM MQ Klienti zvyšují dostupnost aplikací

Programy produktu IBM MQ MQI client se mohou připojovat k různým správcům front ve skupině správců front na základě dostupnosti správce front, vah připojení a afinit. Spuštěním aplikace na jiném počítači než ten, na kterém běží správce front, můžete zlepšit celkovou dostupnost řešení tak dlouho, dokud existuje způsob opětovného připojení aplikace, pokud je instance správce front připojená k selhání.

Skupiny správců front se používají ke zvýšení dostupnosti klienta odpojením klienta od správce front, který je zastaven, a vyrovnavání zátěže klienta v rámci skupiny správců front, spíše jako sprejer IP. Klientská aplikace nesmí mít žádné afinity s nezdařeným správcem front, jako je například závislost na konkrétní frontě, nebo nemůže pokračovat ve zpracování.

Automatické opětovné připojení klientů a správce front s více instancemi zvyšují dostupnost klientů tím, že řeší některé problémy s afinitou. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Můžete nastavit volbu MQCNO MQCNO_RECONNECT_Q_MGR, chcete-li přinutit klienta, aby se znovu připojil ke stejnému správci front:

1. Pokud dříve připojený správce front instance není spuštěn, pokus o připojení se znovu pokusí, dokud nebude správce front spuštěn znovu.
2. Je-li správce front konfigurován jako správce front s více instancemi, pak se klient znovu připojí k aktivní instanci.

Po automatickém opětovném připojení ke stejnému správci front byla obnovena velká část informací o stavu, které správce front v zastoupení klienta držel, například fronty, které byly otevřeny, a téma, k jehož odběru bylo přihlášeno, obnoveno. Pokud klient otevřel dynamickou odpověď-do fronty pro přijetí odpovědi na požadavek, je obnoveno připojení k frontě pro odpověď.

Ujištění se, že zprávy nejsou ztraceny (protokolování)

Příkaz IBM MQ zaznamenává všechny významné změny trvalých dat řízených správcem front v protokolu pro zotavení.

To zahrnuje vytváření a odstraňování objektů, trvalé aktualizace zpráv, stavy transakcí, změny atributů objektů a aktivity kanálu. Protokol obsahuje informace, které potřebujete k obnově všech aktualizací do front zpráv pomocí:

- Uchovávání záznamů o změnách správce front
- Uchovávání záznamů aktualizací fronty pro použití procesem restartování
- Povolení obnovy dat po selhání hardwaru nebo softwaru

Produkt IBM MQ se však také spoléhá na diskový systém, který je hostitelem jeho souborů, včetně souborů protokolu. Je-li diskový systém sám o sobě nespolehlivý, mohou být informace, včetně informací o protokolu, ztraceny.

Jaké protokoly vypadají jako

Protokoly se skládají z primárních a sekundárních souborů a řídicího souboru. Definujete počet a velikost souborů protokolu a umístění, kde jsou uloženy v systému souborů.

Protokol IBM MQ se skládá ze dvou komponent:

1. Jeden nebo více souborů dat protokolu.
2. Řídicí soubor protokolu

Soubor dat protokolu je také znám jako oblast protokolu.

Existuje mnoho oblastí protokolu, které obsahují zaznamenaná data. Můžete definovat počet a velikost (jak je vysvětleno v části [“Předvolby protokolu pro IBM MQ”](#) na stránce 100), nebo provést výchozí nastavení systému tří primárních a dvou sekundárních fyzických oblastí.

Každá ze tří primárních a dvou sekundárních oblastí pro rozšíření je standardně 16 MB.

Při vytvoření správce front je počet předem přidělených rozsahů protokolu k počtu přidělených oblastí *primární* oblasti protokolu. Pokud číslo nezádáte, použije se výchozí hodnota.

Produkt IBM MQ používá dva typy protokolování:

- Kruhový
- Lineární

Počet oblastí protokolu použitých s lineárním protokolováním může být velmi velký, v závislosti na frekvenci záznamu obrazu média.

Další informace viz [“Typy protokolování”](#) na stránce 458.

Pokud jste v produktu IBM MQ for Windows nezměnili cestu k protokolu, dojde k vytvoření oblastí protokolu v adresáři:

```
C:\ProgramData\IBM\MQ\log\
```

Pokud jste v produktu IBM MQ for SYSTÉM UNIX a Linux nezměnili cestu k protokolu, vytvoří se oblastí pro rozšíření protokolu pod adresářem:

```
/var/mqm/log/
```

IBM MQ začíná s těmito oblastmi primárního protokolu, ale pokud není primární prostor žurnálu dostatečný, alokuje *sekundární* oblasti protokolu pro rozšíření. To dělá dynamicky a odstraňuje je, když se sníží poptávka po protokolovaných prostorech. Standardně může být alokováno až dva rozšíření sekundárních protokolů. Tuto výchozí alokaci můžete změnit, jak je popsáno v tématu [“Změna konfiguračních informací IBM MQ a správce front”](#) na stránce 81.

Soubor řízení žurnálu

Řídicí soubor protokolu obsahuje informace potřebné k popisu stavu fyzických oblastí protokolu, jako je jejich velikost a umístění, a název další dostupné oblasti.

Důležité: Řídicí soubor protokolu je určen pouze pro interní použití správce front.

Správce front uchovává řídicí data přidružená ke stavu protokolu pro zotavení v řídicím souboru protokolu a vy nesmíte upravit obsah řídicího souboru protokolu.

Řídicí soubor protokolu se nachází v cestě k protokolu a nazývá se `amqh1ctl.1fh`. Při zálohování nebo obnově vašeho správce front se ujistěte, že je soubor řízení protokolu zálohován a obnoven spolu s oblastmi protokolu.

Typy protokolování

V produktu IBM MQ existují dva způsoby udržování záznamů o aktivitách správce front: kruhové protokolování a lineární protokolování.

Kruhové protokolování

Použijte kruhové protokolování, pokud chcete, aby obnova restartoval, použijte protokol k odvolání transakcí, které probíhaly, když se systém zastavil.

Kruhové protokolování zachová všechna data restartování v kruhu souborů protokolu. Protokolování vyplní první soubor v kruhu a poté vždy přejde na další, dokud nejsou naplněny všechny soubory. Nakonec přejde na první soubor v kruhu a začne znovu. Tento postup probíhá po celou dobu používání protokolu a má výhodu, že nikdy nedojde k nedostatku souborů protokolu.

Produkt IBM MQ uchovává záznamy protokolu vyžadované k restartování správce front bez ztráty dat, dokud tyto záznamy nebudou nadále vyžadovány k zajištění zotavení dat správce front. Mechanismus pro

uvolnění souborů protokolu pro opětovné použití je popsán v tématu [“Restartovat obnovu”](#) na stránce 460.

lineární protokolování

Použijte lineární protokolování, chcete-li jak obnovu znovuspuštění, tak obnovu médií (opětovné vytvoření ztracených nebo poškozených dat opětovným přehráváním obsahu protokolu). Lineární protokolování uchovává protokolovaná data v souvislé posloupnosti souborů protokolu.

Soubory protokolu mohou být volitelně:

- Opětovné použití, ale pouze v případě, že již nejsou potřebné k restartování obnovy nebo zotavení média.
- Ručně archivováno pro dlouhodobé uložení a analýzu.

Frekvence obrazů médií určuje, kdy lze znovu použít lineární soubory protokolu, a je hlavním faktorem toho, kolik místa na disku musí být k dispozici pro lineární soubory protokolů.

Správce front můžete nakonfigurovat tak, aby automaticky přijal pravidelné obrazy médií, a to buď na základě času, nebo využití protokolu, nebo můžete obrazy médií naplánovat ručně.

Váš administrátor rozhodne, jaká zásada se má implementovat, a důsledky na využití prostoru na disku. Soubory žurnálu potřebné pro restart musí být vždy dostupné, zatímco soubory protokolů potřebné pouze pro obnovu médií lze archivovat do delšího termínu úložiště, například z pásky.

Pokud administrátor povolí automatickou správu protokolů a automatické obrazy média, bude se lineární protokolování chovat podobně jako velmi velký kruhový protokol, ale s vyšší redundancí proti selhání média umožněným obnovou médií.

Aktivní protokol

Existuje celá řada souborů, které se říká, že jsou *aktivní* v obou lineárních a kruhových protokolování. Aktivní protokol je maximální množství protokolovacího prostoru, ať už používáte kruhové nebo lineární protokolování, které může být odkazováno restartováním nápravy.

Počet aktivních souborů protokolu je obvykle menší než počet primárních souborů protokolu, jak je definováno v konfiguračních souborech. (Informace o definování čísla naleznete v tématu [“Výpočet velikosti protokolu”](#) na stránce 463 .)

Všimněte si, že aktivní protokolovací prostor nezahrnuje prostor potřebný pro obnovu médií a že počet souborů protokolu použitých s lineárním protokolováním může být velmi velký, v závislosti na toku zpráv a frekvenci obrazů médií.

Neaktivní protokol

Není-li již soubor protokolu potřebný pro obnovení po restartování, stane se z něj *inactive*. Soubory protokolu, které nejsou povinné pro obnovu po restartu, nebo obnovu médií, lze považovat za nadbytečné soubory protokolu.

Při použití automatického správy protokolů správce front řídí zpracování těchto zbytečných souborů protokolu. Pokud jste zvolili ruční správu protokolů, stává se odpovědností administrátora spravovat (například odstraňovat a archivovat) nadbytečné soubory žurnálu, pokud již nejsou pro vaši operaci zajímavé.

Další informace o odebírání souborů protokolu naleznete v příručce [“Správa protokolů”](#) na stránce 467 .

Soubory sekundárního protokolu

Ačkoli jsou sekundární soubory protokolů definovány pro lineární protokolování, nejsou použity v běžném provozu. Pokud se vyskytne situace, kdy, pravděpodobně kvůli dlouhodobým transakcím, není možné uvolnit soubor z aktivního fondu, protože to může být stále potřeba pro restart, sekundární soubory jsou formátovány a přidány do aktivního fondu souborů protokolu.

Pokud je použit počet sekundárních souborů, které jsou k dispozici, požadavky na většinu dalších operací vyžadujících aktivitu protokolu budou odmítnuty s návratovým kódem MQRC_RESOURCE_PROBLEM vráceným do aplikace a všechny přerušitelné transakce budou zvažovány pro asynchronní odvolání transakce.



Upozornění: Oba typy protokolování se mohou vypořádat s neočekávanou ztrátou výkonu za předpokladu, že nedošlo k žádnému selhání hardwaru.

Restartovat obnovu

Jak kruhové protokolování, tak i správci front s lineárním protokolováním podporují opětovné spuštění zotavení. Bez ohledu na to, jak neočekávaně skončí předchozí instance správce front (například výpadek proudu) při restartu správce front, obnoví svůj trvalý stav do správného transakčního stavu v místě ukončení.

Restart obnovy závisí na zachování integrity disku. Podobně operační systém by měl zajistit integritu disku bez ohledu na to, jak nečekaně může dojít k ukončení operačního systému.

V případě velmi neobvyklé události, že integrita disku není udržována, poskytuje lineární protokolování (a obnova médií) další možnosti redundance a možností zotavení. Se stále více běžnými technologiemi, jako je RAID, je čím dál vzácnější a trpí problémy s integritou disků a mnoho podniků konfiguruje kruhové protokolování a používá pouze obnovu restartu.

IBM MQ je navržen jako klasický správce prostředků protokolování zápisu dopředu. Trvalé aktualizace front zpráv probíhá ve dvou fázích:

1. Záznamy protokolu představující aktualizaci jsou zapsány spolehlivě do protokolu pro zotavení
2. Soubor fronty nebo vyrovnávací paměti jsou aktualizovány způsobem, který je pro váš systém nejefektivnější, ale nemusí být nutně konzistentně konzistentní.

Soubory protokolu se tak mohou stát aktuálnější než základní vyrovnávací paměť fronty a stav souboru.

Pokud by tato situace mohla pokračovat, je třeba velmi velký objem přehrávání protokolu, aby byl stav fronty konzistentní po zotavení z havárie.

IBM MQ používá checkpoints, aby se omezil objem přehrávání protokolu, který se požaduje po zotavení z havárie. Klíčová událost, která řídí, zda je soubor protokolu označen jako aktivní nebo ne, je checkpoint.

Kontrolní bod IBM MQ je bod:

- Konzistentnosti mezi protokolem o zotavení a soubory objektů.
- To identifikuje místo v protokolu, z něhož je zaručeno přehrávání následujících záznamů protokolu pro obnovení fronty do správného logického stavu v době, kdy mohl správce front skončit.

Během kontrolního bodu IBM MQ vyprázdni starší aktualizace do souborů fronty podle potřeby, aby bylo možné omezit objem záznamů žurnálu, které je třeba přehrát, aby se fronty vraly zpět do konzistentního stavu po obnově po havárii.

Poslední dokončený kontrolní bod označuje bod v protokolu, ze kterého musí být přehrán přehrávání během zotavení z havárie. Frekvence kontrolního bodu je tedy odvoláním mezi režii záznamu kontrolních bodů a zvýšením potenciálního času obnovy odvozeného z těchto kontrolních bodů.

Pozice v protokolu spuštění posledního dokončovacího kontrolního bodu je jedním z klíčových faktorů pro určení, zda je soubor protokolu aktivní nebo neaktivní. Dalším klíčovým faktorem je pozice v protokolu prvního záznamu protokolu vztahující se k první trvalé aktualizaci provedené aktuální aktivní transakcí.

Je-li nový kontrolní bod zaznamenán ve druhém nebo novějším souboru protokolu a žádná aktuální transakce se neodkazuje na záznam protokolu v prvním souboru protokolu, první soubor protokolu se stane neaktivním. V případě kruhového protokolování je nyní první soubor protokolu připraven k opětovnému použití. V případě lineárního protokolování se první soubor protokolu obvykle požaduje pro obnovu médií.

Pokud nakonfigurujete buď kruhové protokolování, nebo automatickou správu protokolu, správce front bude spravovat neaktivní soubory protokolu. Pokud nakonfigurujete lineární protokolování pomocí ruční

správy protokolů, stane se administrativní úlohou pro správu neaktivních souborů podle požadavků vaší operace.

Produkt IBM MQ generuje kontrolní body automaticky. Tato opatření se přijímají, pokud:

- Spustí se správce front.
- Při ukončení práce
- Když je protokolovací prostor nízký
- **distributed** Po provedení předchozího kontrolního bodu bylo zaprotokolováno 50 000 operací.
- **z/OS** Pro produkt z/OSurčuje nastavení LOGLOAD počet operací v kontrolním bodu.

Když se IBM MQ znovu spustí, najde v protokolu nejnovější záznam kontrolního bodu. Tyto informace jsou uloženy v souboru kontrolního bodu, který je aktualizován na konci každého kontrolního bodu. Všechny operace, k jejichž provedení došlo od kontrolního bodu, se přehrávají vpřed. To je známo jako fáze přehrání.

Fáze přehrávání vrací fronty zpět do logického stavu, ve kterém byly před selháním systému nebo ukončením běhu systému. Během fáze přehrávání je vytvořen seznam transakcí, které byly prolet při selhání systému nebo k ukončení práce systému.

distributed Vydávají se zprávy AMQ7229 a AMQ7230 , které označují průběh fáze přehrávání.

Chcete-li zjistit, které operace mají být odvráceny nebo potvrzeny, IBM MQ přistupuje ke každému aktivnímu záznamu protokolu přidruženému k transakci v rámci letu. Tento stav je znám jako fáze obnovení.

distributed Zprávy AMQ7231, AMQ7232 a AMQ7234 jsou vydávány s cílem označit průběh fáze obnovení.

Jakmile jsou k dispozici všechny potřebné záznamy protokolu během fáze obnovy, každá aktivní transakce se zase vyřeší a každá operace přidružená k transakci bude buď vrácena, nebo potvrzena. To je známo jako fáze řešení.

distributed Byla vydána zpráva AMQ7233 , která označuje průběh fáze rozpoznání.

z/OS V systému z/OSse zpracování restartu skládá z různých fází.

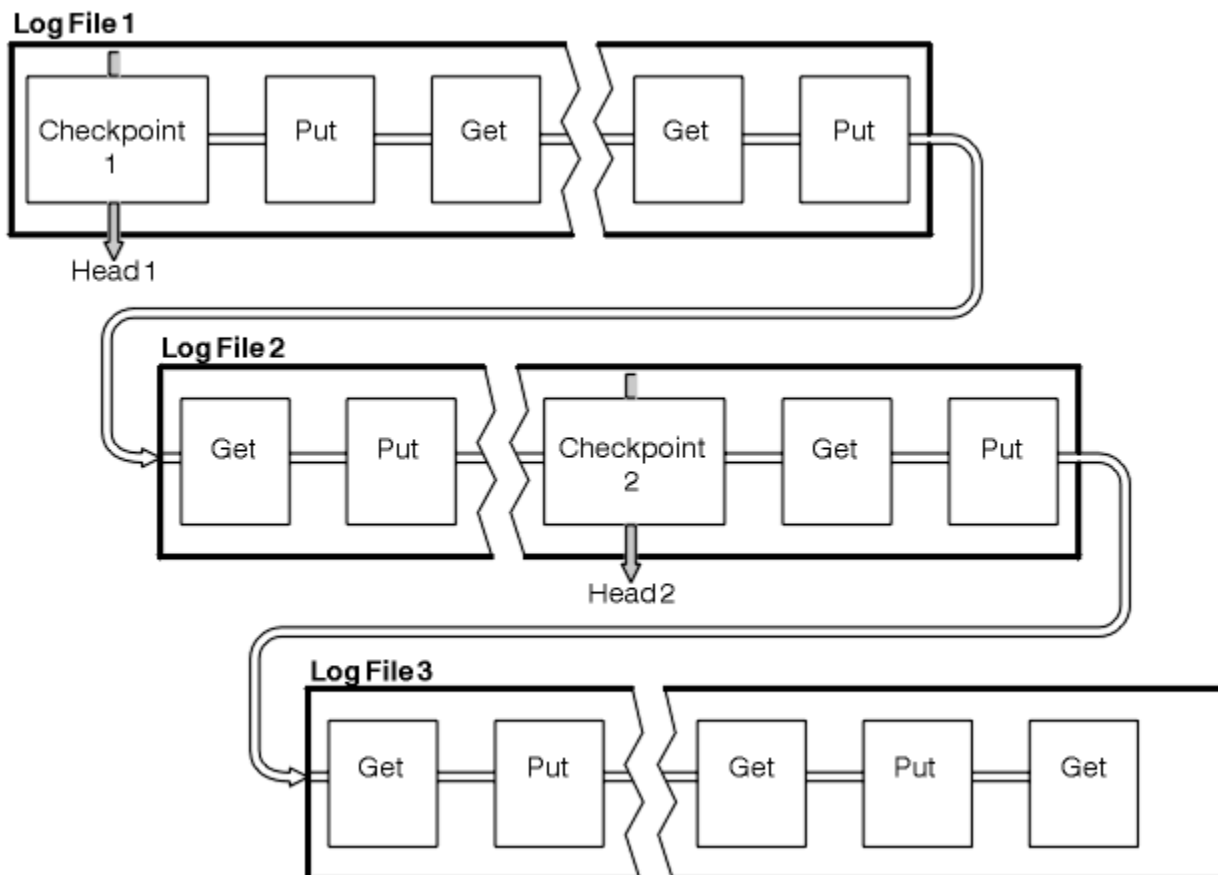
1. Rozsah protokolu pro zotavení je založen na obnově médií požadovaných pro sady stránek a na nejstaršímu záznamu protokolu, který je nezbytný pro zálohování jednotek práce a získání zámeků pro nejisté jednotky práce.
2. Jakmile je určen rozsah protokolu, je dopředné čtení protokolu prováděno tak, aby stránka byla nastavena na nejnovější stav, a také uzamknout všechny zprávy související s neověřeným nebo neověřeným pracovním jednotkám.
3. Po dokončení dopředného čtení protokolů jsou protokoly čteny zpět, aby se vymkly veškeré jednotky práce, které byly v době selhání za letu nebo v době selhání.

z/OS Příklad zpráv, které se mohou zobrazit:

```
CSQR001I +MQOX RESTART INITIATED
CSQR003I +MQOX RESTART - PRIOR CHECKPOINT RBA=00000001E48C0A5E
CSQR004I +MQOX RESTART - UR COUNTS - 806
IN COMMIT=0, INDOUBT=0, INFLIGHT=0, IN BACKOUT=0
CSQR030I +MQOX Forward recovery log range 815
from RBA=00000001E45FF7AD to RBA=00000001E48C1882
CSQR005I +MQOX RESTART - FORWARD RECOVERY COMPLETE - 816
IN COMMIT=0, INDOUBT=0
CSQR032I +MQOX Backward recovery log range 817
from RBA=00000001E48C1882 to RBA=00000001E48C1882
CSQR006I +MQOX RESTART - BACKWARD RECOVERY COMPLETE - 818
INFLIGHT=0, IN BACKOUT=0
CSQR002I +MQOX RESTART COMPLETED
```

Poznámka: Pokud existuje velké množství protokolu, které má být přečten, zprávy CSQR031I (dopředné zotavení) a CSQR033I (zpětné zotavení) jsou vydávány pravidelně pro zobrazení postupu.

V produktu Obrázek 80 na stránce 462 již nejsou všechny záznamy před posledním kontrolním bodem, kontrolním bodem 2, již IBM MQ vyžadovány. Fronty je možné obnovit z informací o kontrolním bodu a všech pozdějších položek protokolu. Pro kruhové protokolování se všechny uvolněné soubory před kontrolním bodem mohou znovu použít. V případě lineárního protokolu se uvolněné soubory protokolu již nemusí zpřístupnit pro normální provoz a stát se neaktivními. V tomto příkladu se ukazatel hlavy fronty přesune na poslední kontrolní bod kontrolního bodu 2, který se pak stane novou hlavou fronty, hlava 2. Soubor protokolu 1 lze nyní znovu použít.



Obrázek 80. Ukládám

Kontrola s dlouhotrvajícími transakcemi

Jak dlouho běžící transakce ovlivňuje opětovné použití souborů protokolu.

Příkaz Obrázek 81 na stránce 463 zobrazuje, jak dlouho běžící transakce ovlivňuje opětovné použití souborů protokolu. V tomto příkladu provedla transakce s dlouhou dobou zpracování záznam do protokolu, zobrazený jako LR 1, po prvním zobrazení kontrolního bodu. Transakce se nedokončila (v bodě LR 2) až po třetím kontrolním bodu. Všechny informace z protokolu od LR 1 jsou uchovány, aby umožnily obnovu této transakce, je-li to nezbytné, dokud nebude dokončena.

Po dokončení transakce s dlouhou dobou zpracování v LR 2 se hlava protokolu logicky přesune do kontrolního bodu 3, nejnovější zaprotokolovaný kontrolní bod. Soubory obsahující záznamy protokolu před kontrolním bodem 3, hlava 2, již nejsou potřebné. Používáte-li kruhové protokolování, lze prostor znovu použít.

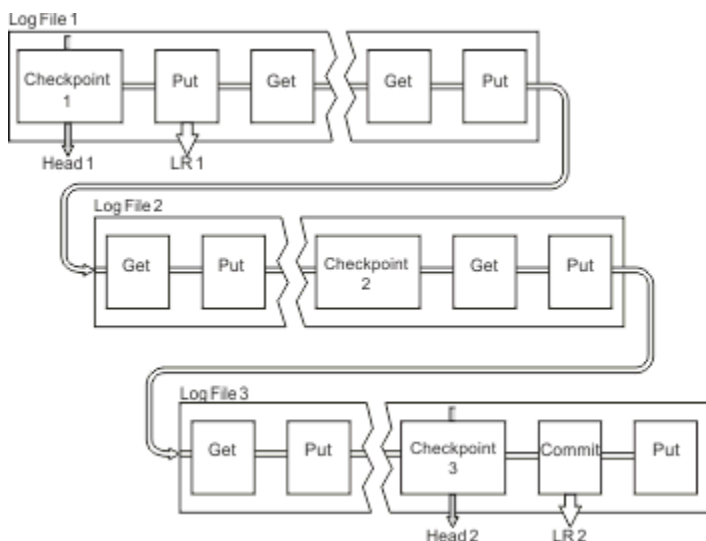
Pokud jsou primární soubory žurnálu zcela zaplněna před dokončením transakce s dlouhou dobou zpracování, mohou být použity sekundární soubory protokolu, aby nedošlo k zaplnění protokolů.

Aktivity, které jsou zcela pod kontrolou správce front, například checkpointing, jsou naplánovány, aby se pokusila udržet aktivitu v rámci primárního protokolu.

Je-li však pro podporu chování mimo kontrolu správce front vyžadován sekundární prostor žurnálu (například doba trvání jedné z vašich transakcí), správce front se pokusí použít definovaný sekundární protokolovací prostor, aby mohla být tato aktivita dokončena.

Pokud se tato aktivita nedokončí do doby, kdy se používá 80% celkového prostoru protokolu, správce front zahájí akci pro uvolnění protokolovacího prostoru bez ohledu na to, že má dopad na aplikaci.

Když se hlava protokolu přesune a používáte kruhové protokolování, mohou být primární soubory protokolu vhodné k opětovnému použití a modul protokolování po vyplnění aktuálního souboru znovu použije první primární soubor, který je k dispozici. Pokud používáte lineární protokolování, hlavička protokolu je stále přesunuta dolů do aktivního fondu a první soubor se stane neaktivní. Nový primární soubor je formátován a přidán do spodní části fondu v připravenosti pro budoucí aktivity protokolování.



Obrázek 81. Kontrola s dlouhotrvající transakcí

Výpočet velikosti protokolu

Odhadování velikosti protokolu, které správce front potřebuje.

Po rozhodnutí, zda správce front používá kruhové nebo lineární protokolování, je třeba odhadnout velikost Aktivní protokol, který správce front potřebuje. Velikost aktivního žurnálu se určuje podle následujících konfiguračních parametrů protokolu:

LogFilePages

Velikost každého primárního a sekundárního souboru protokolu v jednotkách stránek 4K

LogPrimaryFiles

Počet předem přidělených primárních souborů protokolu

LogSecondaryFiles

Počet sekundárních souborů protokolu, které lze vytvořit pro použití při zaplnění primárních souborů protokolu

Notes:

1. Můžete změnit počet primárních a sekundárních souborů protokolu při každém spuštění správce front, ačkoli si nemusíte všimnout efektu změny, kterou jste provedli na sekundárních protokolech, okamžitě.
2. Velikost souboru protokolu nelze změnit. Před vytvořením správce front je třeba určit **před** vytvořením správce front.
3. Počet primárních souborů protokolu a velikost souboru protokolu určují velikost prostoru protokolu, který je předem přidělen při vytvoření správce front.
4. Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 511 na systémech SYSTÉM UNIX a Linux nebo 255 na Windows, který za přítomnosti dlouho běžících transakcí omezuje

maximální velikost protokolovacího prostoru dostupného správci front pro opětovné spuštění zotavení. Množství protokolovacího prostoru, které správce front potřebuje pro obnovu médií, tento limit nesdílí.

5. Je-li používáno *kruhové* protokolování, správce front znovu použije primární a sekundární protokolovací prostor. Správce front bude až do limitu alokovat sekundární soubor protokolu, když se soubor protokolu zaplní, a další primární soubor protokolu v posloupnosti nebude k dispozici.

Informace o počtu protokolů, které je třeba přidělit, naleznete v příručce [“Jak velký mám udělat svůj aktivní protokol?”](#) na stránce 464 . Oblasti primárního protokolu se používají v pořadí a tato posloupnost se nezmění.

Například, pokud máte tři primární protokoly 0, 1a 2, pořadí použití je 0,1,2 následované 1,2,0, 2,0,1, zpět na 0,1,2 atd. Všechny sekundární protokoly, které jste přidělili, jsou prosouzeni podle potřeby.

6. Primární soubory protokolu jsou k dispozici pro opětovné použití během kontrolního bodu. Před přijetím kontrolního bodu správce front vezme v úvahu jak primární, tak sekundární protokolovací prostor, protože velikost prostoru žurnálu je nízká.

Další informace viz [“Předvolby protokolu pro IBM MQ”](#) na stránce 100.

Jak velký mám udělat svůj aktivní protokol?

Odhadování velikosti aktivního protokolu, který správce front potřebuje.

Velikost aktivního žurnálu je omezena:

```
logsize = (primaryfiles + secondaryfiles) * logfilepages * 4096
```

Protokol by měl být dostatečně velký, aby se mohl vypořádat s nejdelší spuštěnou transakcí spuštěnou v okamžiku, kdy správce front zapisuje maximální množství dat za sekundu na disk.

Pokud vaše nejdelší běžící transakce běží na N sekund a maximální množství dat za sekundu zapsaných na disk správcem front je B bajtů za sekundu v protokolu, váš protokol by měl být alespoň:

```
logsize >= 2 * (N+1) * B
```

Správce front bude pravděpodobně zapisovat maximální množství dat za sekundu na disk, pokud pracujete v pracovní zátěži, nebo může být při záznamu obrazů médií.

Pokud je transakce spuštěna tak dlouho, že oblast protokolu obsahující svůj první záznam protokolu není obsažena v aktivním protokolu, správce front odvolá aktivní transakce jeden po druhém, počínaje transakcí s nejstarším záznamem protokolu.

Správce front musí před použitím maximálního počtu primárních a sekundárních souborů deaktivovat staré oblasti pro rozšíření protokolu a správce front musí přidělit další oblast protokolu.

Rozhodněte se, jak dlouho má trvat nejdéle běžící transakce, než bude správce front povolen návrat zpět. Vaše nejdelší běžící transakce může čekat na pomalý provoz sítě nebo, v případě špatně navržené transakce, čekat na vstup uživatele.

Zadáním následujícího příkazu **runmqsc** můžete zjistit, jak dlouho se nejdéle běžící transakce spouští:

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

Vydáním příkazu `dspmqt:n` -a se zobrazí všechny příkazy XA a non XA ve všech stavech.

Vydáním tohoto příkazu vypíše datum a čas, kdy byl zapsán první záznam protokolu pro všechny vaše aktuální transakce.



Upozornění: Pro účely výpočtu velikosti protokolu se jedná o čas od okamžiku, kdy byl zapsán první záznam protokolu, a nikoli čas od spuštění aplikace nebo transakce. Zaokrouhlit délku nejdéle běžící transakce na nejbližší sekundu. Je to způsobeno optimalizací ve správci front.

První záznam protokolu může být zapsán dlouho po spuštění aplikace, pokud aplikace začíná například zadáním volání MQGET, které čeká po určitou dobu, než se skutečně dostane zprávy.

Přezkoumáním maximálního sledovaného data a času výstupem z


```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

command you issued originally, from the current date and time, you can estimate how long your long along running transaction runs.

Ujistěte se, že jste spustili tento příkaz **runmqsc** opakovaně, zatímco nejdéle běžící transakce jsou spuštěny ve špičce pracovní zátěže, abyste nepodceňovali délku nejdelší spuštěné transakce.

V produktu IBM MQ 8.0 lze používat nástroje operačního systému, například **iostat** na platformách UNIX .

Například, pokud nástroje operačního systému ukazují, že logické bajty za sekundu zapsané do protokolu jsou přibližně 12 MB za sekundu, pomocí:

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

ukazuje, že nejdelší běžící transakce byla:

```
CONN(57E14F6820700069)
EXTCONN(414D51436D61726B2020202020202020)
TYPE(CONN)
APPLTAG(msginteg_r)                UOWLOGDA(2016-09-20)
UOWLOGTI(16.44.14)
```

Jako aktuální datum a čas byl 2016-09-20 16.44.19, tato transakce byla spuštěna po dobu 5 sekund. Je však nutné tolerovat transakce trvající 10 sekund, než je správce front odvolá zpět. Velikost protokolu by proto měla být následující:

```
2 * (10 + 1) * 12 = 264 MB
```

Je-li použita předvolba **LogFilePages** , která je 4096, musíte se ujistit, že součet vašich **LogPrimaryFiles** a **LogSecondaryFiles** je nejméně 17:

```
264 MB < 17 * 4096 * 4096
```

Pokud velikost protokolu zadáte tak, aby se očekávaná pracovní zátěž spouštělo v rámci primárních souborů, postupujte takto:

- Sekundární soubory poskytují určitou rezervu v případě, že je potřeba dodatečný prostor protokolu.
- Kruhové protokolování vždy používá předem přidělené primární soubory, což je okrajově rychlejší než přidělování a dealokace sekundárních souborů.
- Správce front používá pouze zbývající prostor v primárních souborech k výpočtu, kdy má být použit další kontrolní bod.

Proto v předchozím příkladu nastavte následující hodnoty:

- **LogFilePages** = 4096
- **LogPrimaryFiles** = 17
- **LogSecondaryFiles** = 5

Všimněte si následujícího:

- V tomto příkladě 5 sekundářů je o více než 20% aktivního protokolovacího prostoru.

Měli byste si být vědomi toho, že správce front podniká kroky ke snížení využití protokolovacího prostoru, pokud se používá více než 80% celkového prostoru protokolu.

- Proveďte stejný výpočet, ať už používáte lineární nebo kruhové protokolování.

Nezáleží na tom, zda vypočítáte velikost lineárního nebo kruhového aktivního protokolu, protože koncept aktivního protokolu znamená stejný jak v lineárním, tak i v kruhové protokolování.

- Oblasti protokolu potřebné pro obnovení médií nejsou v aktivním protokolu, a proto se nezapočítávají do počtu primárních a sekundárních souborů.

Co se stane, když udělám svůj protokol příliš malý?

Body, které byste měli zvážit při odhadu minimální velikosti protokolu.

Pokud je váš protokol příliš malý:

- Dlouho běžící transakce budou vráceny zpět.
- Může vám dojít k tomu, že protokol FFDC vás informuje o tom, že protokol je příliš malý.
- Další kontrolní bod se chce spustit dříve, než se předchozí kontrolní bod ukončí.

Důležité: Bez ohledu na to, jak přesně odhadujete velikost vašeho protokolu, zachovávají se integrity dat.

Vysvětlení kontrolních bodů viz [“Restartovat obnovu”](#) na stránce 460 . Pokud se velikost protokolovacího prostoru, který zbývá v oblastech aktivního protokolu, stává krátkou, správce front naplánuje kontrolní body častěji.

Kontrolní bod zabere určitý čas; není okamžitý. Čím více dat je třeba zaznamenat do kontrolního bodu, tím déle bude kontrolní bod trvat. Pokud se protokol malých kontrolních bodů může překrývat, znamená to, že další kontrolní bod je požadován dříve, než skončí předchozí kontrolní bod. Pokud se tato chyba vyskytne, jsou zapsány chybové zprávy.

Pokud dojde k překryvu dlouhých spuštěných transakcí nebo se kontrolní body překrývají, bude správce front pokračovat ve zpracování pracovní zátěže. Krátkodobé transakce jsou nadále spuštěné jako normální.

Správce front však není spuštěn optimálně a výkon může být snížen. Měli byste restartovat správce front s dostatkem protokolovacího prostoru.

Co se stane, pokud se můj protokol příliš velký?

Body, které byste měli zvážit při odhadu maximální velikosti protokolu.

Pokud je váš protokol příliš velký:

- Můžete zvýšit čas potřebný k nouzovému restartu, i když je to nepravděpodobné.
- Používáte zbytečný prostor na disku.
- Velmi dlouho běžící transakce je tolerována.

Důležité: Bez ohledu na to, jak přesně odhadujete velikost vašeho protokolu, zachovávají se integrity dat.

Popis způsobu, jakým správce front čte protokol při restartování, naleznete v tématu [“Restartovat obnovu”](#) na stránce 460 . Správce front přehraje protokol z posledního kontrolního bodu a poté vyřeší všechny transakce, které byly aktivní v okamžiku, kdy byl ukončen správce front.

Při řešení transakce správce front načte zpět všechny záznamy protokolu přidružené k dané transakci. Tyto záznamy protokolu mohou přededat poslední kontrolní bod.

Při přidělení velmi rozsáhlého protokolu správce front přidělujete správci front oprávnění ke čtení každého záznamu žurnálu v protokolu při restartu, ačkoli obvykle správce front toto nemusí provést. Potenciálně, v nepravděpodobném případě, že by se to stalo, tento proces by mohl trvat dlouho.

Pokud před ukončením správce front došlo k neočekávanému ukončení kontroly před koncem správce front, výrazně se prodlužuje doba restartování správce front s velkým protokolem. Omezení velikosti protokolu omezuje dobu spuštění nouzového restartu.

Abyste se vyhnuli těmto problémům, měli byste zajistit, že:

- Vaše pracovní zátěž se může pohodlně vejít do protokolu, který není příliš velký.
- Vyhýbejte se přerušitelných transakcím.

Správa protokolů

Chcete-li spravovat lineární protokoly, musíte se sami spravovat. Avšak kruhové protokoly jsou téměř samoobslužné, ale někdy potřebují zásah k vyřešení problémů s prostorem.

Při kruhové protokolování získá správce front uvolněný prostor v souborech protokolu. Tato aktivita není uživateli zřejmá a obvykle se nezobrazuje velikost použitého místa na disku, protože přidělený prostor se rychle znovu použije.

V případě lineárního protokolování se může protokol vyplnit, pokud nebyl kontrolní bod dlouho pořízen, nebo pokud dlouho běžící transakce zapsala záznam protokolu před dlouhou dobou. Správce front se pokusí přijímat kontrolní body často natolik, aby se předešlo prvnímu problému.

distributed Pokud se protokol zaplní, je vydána zpráva AMQ7463 . Kromě toho, pokud se protokol zaplní, protože dlouho běžící transakce zabránila uvolnění prostoru, vydá se zpráva AMQ7465 .

Ze záznamů protokolu jsou pro restartování správce front potřebné pouze ty, které byly zapsány od posledního dokončovacího kontrolního bodu a ty, které jsou zapsány v rámci aktivních transakcí.

V průběhu času se nejstarší záznamy protokolu nestanou zbytečnými pro restartování správce front.

Je-li zjištěna dlouhodobě spuštěná transakce, aktivita je naplánována k asynchronnímu odvolání transakce. Pokud z nějakého neočekávaného důvodu došlo k selhání asynchronní operace rollback, některá volání MQI v této situaci vrátí funkci MQRC_RESOURCE_PROBLEM.

Všimněte si, že prostor je vyhrazen pro potvrzení nebo odvolání všech vnitřních transakcí, takže MQCMIT nebo MQBACK by neměly selhat.

Správce front odvolá transakce, které se spouští po dlouhou dobu. Aplikace, která má transakci, je odvolána tímto způsobem, nemůže provést následné operace MQPUT nebo MQGET , které určují synchronizační bod pod stejnou transakcí.

Transakce však skončily ručním spuštěním nového protokolu. Všimněte si, že zatímco nový protokolovací prostor je alokován okamžitě, prostor protokolu, který byl uvolněn, trvá konečný čas, aby byl uvolněn.

Pokus o vložení nebo získání zprávy pod bodem synchronizace v tomto stavu vrátí MQRC_BACKED_OUT. Aplikace pak může vydat příkaz MQCMIT , který vrátí MQRC_BACKED_OUT nebo MQBACK a spustí novou transakci. Po odvolání transakce, která spotřebovává příliš mnoho prostoru žurnálu, dojde k uvolnění protokolovacího prostoru a správce front bude i nadále fungovat normálně.

Co se stane, když se disk zaplní

Komponenta protokolování správce front se může vypořádat s celým diskem a s úplnými soubory protokolu. Pokud se disk obsahující protokol zaplní, vydá správce front zprávu AMQ6709 a provede se záznam o chybě.

Soubory protokolu se vytvářejí ve své pevné velikosti a nejsou rozšířeny, aby se do nich zapisovány záznamy protokolu. To znamená, že produkt IBM MQ může nedostatek prostoru na disku spustit pouze v případě, že vytváří nový soubor. Při zápisu záznamu do protokolu nemůže dojít k nedostatku místa. Produkt IBM MQ vždy ví, kolik místa je k dispozici v existujících souborech protokolu, a spravuje prostor v souborech odpovídajícím způsobem.

Pokud vyplníte jednotku obsahující soubory protokolu, můžete být schopni uvolnit některé místo na disku. Pokud používáte lineární protokol, mohou existovat některé neaktivní soubory protokolu v adresáři protokolů a vy můžete tyto soubory zkopírovat na jinou jednotku nebo zařízení.

Kruhové protokolování vrací problém prostředku.

Pokud stále dochází k nedostatku místa, zkontrolujte, zda je konfigurace protokolu v konfiguračním souboru správce front správná. Je možné, že budete moci snížit počet primárních nebo sekundárních souborů protokolu, aby protokol nevyrostl z dostupného místa.

Velikost souborů protokolu pro existujícího správce front nelze změnit. Správce front vyžaduje, aby všechny oblasti žurnálu byly stejné velikosti.

Správa souborů protokolu

Alokujte dostatečný prostor pro vaše soubory protokolů. Pro lineární protokolování můžete odstranit staré soubory protokolu, když již nejsou potřeba.

Informace specifické pro kruhové protokolování

Používáte-li kruhové protokolování, ujistěte se, že je dostatek místa pro uchování souborů protokolu při konfiguraci systému (viz "Předvolby protokolu pro IBM MQ" na stránce 100 a "Protokoly správce front" na stránce 109). Množství prostoru na disku použitého protokolem se nezvýší za nakonfigurovanou velikost, včetně prostoru pro sekundární soubory, které mají být vytvořeny, když je to požadováno.

Informace specifické pro lineární protokolování

Pokud používáte lineární protokol, soubory protokolu se přidávají průběžně, když jsou protokolována data, a velikost použitého prostoru na disku se zvyšuje s časem. Je-li rychlost protokolovaných dat vysoká, prostor na disku se rychle používá v nových souborech protokolu.

V průběhu času se starší soubory protokolu pro lineární protokol již nemusí restartovat správce front nebo provést obnovu médií s jakýmkoli poškozenými objekty. Pro určení, které soubory protokolu jsou stále vyžadovány, jsou tyto metody:

Zprávy událostí modulu protokolování

Když se vyskytne významná událost, například obraz záznamu média, zprávy událostí modulu protokolování se generují. Obsah zpráv událostí modulu protokolování uvádí soubory protokolu, které jsou stále vyžadovány pro restart správce front, a zotavení média. Další informace o zprávách událostí modulu protokolování naleznete v tématu [Události modulu protokolování](#).

Stav správce front

Spuštěním příkazu MQSC, DISPLAY QMSTATUS nebo PCF, Inquire Queue Manager Status, získáte informace o správci front, včetně podrobností o požadovaných souborech protokolu. Další informace o příkazech MQSC, viz [Příkazy skriptu \(MQSC\)](#), a informace o příkazech PCF viz [Automatizace administračních úloh](#).

Zprávy správce front

Správce front pravidelně vydává zprávy s dvojicí zpráv, které indikují, které soubory protokolu jsou potřeba:

- Zpráva AMQ7467I udává název nejstaršího souboru protokolu potřebného k restartování správce front. Tento soubor protokolu a všechny novější soubory protokolu musí být k dispozici během restartování správce front.
- Zpráva AMQ7468I uvádí název nejstaršího souboru protokolu potřebného pro zotavení média.

Chcete-li určit "starší" a "novější" soubory protokolu, použijte místo úpravy, které používá systém souborů, číslo souboru protokolu.

Informace vztahující se na oba typy protokolování

Jsou vyžadovány pouze soubory protokolu vyžadované pro restartování správce front, aktivní soubory protokolů, které jsou online. Neaktivní soubory protokolu lze zkopírovat na archivní médium, jako je například páska pro zotavení z havárie, a odebrat z adresáře protokolů. Neaktivní soubory protokolu, které nejsou povinné pro obnovu médií, mohou být považovány za nadbytečné soubory protokolu. Nepotřebné soubory protokolu můžete odstranit, pokud již nejsou pro vaši operaci zajímavé.

Pokud nelze najít žádný potřebný soubor protokolu, vydá se zpráva AMQ6767E. Vytvořte soubor protokolu a všechny následné soubory protokolu dostupné pro správce front a zkuste operaci zopakovat.

Poznámka: Při provádění obnovy médií musí být všechny požadované soubory žurnálu dostupné v adresáři souborů protokolu v daném okamžiku. Ujistěte se, že jste provedli pravidelné obrazy médií u všech objektů, které byste mohli chtít obnovit, abyste se vyhnuli nedostatku místa na disku pro uchování všech požadovaných souborů protokolu.

Chcete-li například zobrazit obraz média všech objektů ve správci front, spusťte příkaz **rctmqimg**, jak ukazuje následující příklady:

zapWindows

```
rctmqimg -m QMNAME -t all *
```

zapSYSTÉM UNIX a Linux

```
rctmqimg -m QMNAME -t all "*"
```

Spuštění **rctmqimg** přesune pořadové číslo v protokolu médií (LSN) dopředu. Další podrobnosti o pořadových číslech protokolů najdete v tématu [“Výpis obsahu protokolu pomocí příkazu dmpmqlog” na stránce 472](#). **rctmqimg** se nespustí automaticky, proto musí být spuštěn ručně nebo z automatické úlohy, kterou jste vytvořili. Další informace o tomto příkazu naleznete v části **rctmqimg** a **dmpmqlog**.

Poznámka: Zprávy AMQ7467 a AMQ7468 mohou být také vydávány v době spuštění příkazu **rctmqimg**.

Určení nadbytečných souborů protokolu-pouze lineární protokolování

Pro kruhové protokolování nikdy neodstraňujte data z adresáře protokolů. Při správě lineárních souborů protokolů je důležité si být jisti, které soubory mohou být odstraněny nebo archivovány. Tyto informace vám pomohou při provádění tohoto rozhodnutí.

Nepoužívejte čas úpravy systému souborů, abyste určili "starší" soubory protokolu. Použijte pouze číslo souboru protokolu. Použití souborů protokolu správce front je podle složitých pravidel, včetně předalokování a formátování souborů protokolu, dříve než je potřeba. Při pokusu o určení relativního stáří se mohou zobrazit soubory protokolu s časem úpravy, které by byly zavádějící.

K určení nejstaršího potřebného souboru žurnálu jsou k dispozici tři místa, která můžete použít:

- Příkaz DISPLAY QMSTATUS
- Zprávy událostí modulu protokolování a nakonec
- Zprávy protokolu chyb

Pro příkaz DISPLAY QMSTATUS určete nejstarší rozsah protokolu potřebný k:

- Restartujte správce front, zadejte příkaz DISPLAY QMSTATUS RECLOG.
- Proveďte obnovu médií, zadejte příkaz DISPLAY QMSTATUS MEDIALOG.

Obecně platí, že nižší číslo souboru protokolu znamená starší protokol. Pokud nemáte velmi vysoký obrat souboru protokolu, v pořadí 3000 souborů protokolu za den po dobu 10 let, nemusíte obstarávat balení čísel v 9 999 999. V tomto případě můžete archivovat libovolný soubor protokolu s číslem menším než hodnota RECLOG a můžete odstranit libovolný soubor protokolu s číslem menším, než je hodnota RECLOG a MEDIALOG.



Upozornění: The log file wraps, so the next number after 9 999 999 is zero.

Umístění souboru žurnálu

Při výběru umístění pro soubory protokolu pamatujte na to, že operace je výrazně ovlivněna, pokud produkt IBM MQ neformátuje nový protokol z důvodu nedostatku místa na disku.

Používáte-li cyklický protokol, ujistěte se, že na jednotce je dostatek místa pro alespoň konfigurované primární soubory protokolu. Také ponechejte prostor pro alespoň jeden sekundární soubor protokolu, který je potřebný, pokud má protokol růst.

Pokud používáte lineární protokol, umožněte výrazně více prostoru; prostor využitý protokolem se neustále zvyšuje, protože data jsou protokolována.

Měli byste umístit soubory protokolu na samostatnou diskovou jednotku z dat správce front.

Integrita dat na tomto zařízení je prvořadá-měli byste povolit zabudovanou redundanci.

Může být také možné umístit soubory protokolu na více diskových jednotek v zrcadleném uspořádání. To chrání před selháním jednotky, která obsahuje protokol. Bez zrcadlení byste mohli být nuceni vrátit se zpět k poslední záloze vašeho systému IBM MQ .

Použití protokolu pro zotavení

Použití protokolů k zotavení ze selhání.

Existuje několik způsobů, jak mohou být vaše data poškozena. IBM MQ vám pomůže se zotavit z:

- Poškozený datový objekt
- Ztráta napájení v systému
- Selhání komunikace

Tento oddíl se zabývá tím, jak se protokoly používají pro zotavení z těchto problémů.

Obnova ze výpadku proudu nebo selhání komunikace

Příkaz IBM MQ se může zotavit z obou selhání komunikace a ztráty moci. Kromě toho se může někdy zotavit z jiných typů problémů, jako je například neúmyslné odstranění souboru.

V případě selhání komunikace zůstávají trvalé zprávy ve frontách, dokud nejsou odebrány přijímající aplikací. Je-li zpráva přenášena, zůstane v přenosové frontě, dokud ji nebude možné úspěšně přenést. Chcete-li provést obnovu po selhání komunikace, můžete obvykle restartovat kanály pomocí odkazu, který selhal.

If you lose power, when the queue manager is restarted IBM MQ restores the queues to their committed state at the time of the failure. Tím je zajištěno, že žádné trvalé zprávy nebudou ztraceny. Netrvalé zprávy jsou vyřazeny; nepřežijí, když se IBM MQ náhle zastaví.

Obnova poškozených objektů

Existují způsoby, jak může být objekt IBM MQ nepoužitelný, například z důvodu neúmyslného poškození. Pak musíte obnovit buď celý systém, nebo část jeho části. Požadovaná akce závisí na tom, kdy je poškození zjištěno, zda zvolená metoda protokolu podporuje obnovu médií a které objekty jsou poškozené.

Náprava médií

Náprava médií znovu vytváří objekty z informací zaznamenaných v lineárním protokolu. Pokud je například soubor objektu neúmyslně odstraněn nebo je z nějakého jiného důvodu nepoužitelný, obnova médií ji může znovu vytvořit. Informace v protokolu, které se požadují pro obnovu médií objektu, se nazývají *obraz média*.

Obraz média je posloupnost záznamů protokolů, které obsahují obraz objektu, ze kterého lze znovu vytvořit objekt.

První záznam protokolu požadovaný pro opětovné vytvoření objektu je známý jako *záznam o obnově médií* ; je to začátek posledního obrazu média pro objekt. Záznam obnovy médií každého objektu je jednou z částí informací zaznamenaných během kontrolního bodu.

Když je objekt znovu vytvořen z obrazu média, je také nutné přehrát všechny záznamy protokolu popisující aktualizace provedené na objektu od doby, kdy byl naposledy proveden.

Vezměme si například lokální frontu, která má obraz objektu fronty, který byl proveden před tím, než je do fronty vložena trvalá zpráva. Chcete-li znovu vytvořit nejnovější obraz objektu, je třeba přehrávat záznamy protokolu zaznamenávající vložení zprávy do fronty spolu s opětovným přehráváním obrazu.

Když je objekt vytvořen, záznamy v protokolu obsahují dostatek informací k úplnému znovuvytvoření objektu. Tyto záznamy tvoří první obraz média objektu. Poté správce front při každém vypnutí automaticky provede následující záznamy v obrázcích médií:

- Obrázky všech objektů procesu a front, které nejsou lokální
- Obrázky prázdných lokálních front

Obrazy médií lze také zaznamenat ručně pomocí příkazu **rcdmqimg**, který je popsán v souboru [rcdmqimg](#). Tento příkaz zapíše obraz média objektu IBM MQ.

Když byl obraz média zapsán, jsou pro opětovné vytvoření poškozených objektů potřeba pouze protokoly, které obsahují obraz média a všechny protokoly vytvořené po této době. Přínos vytváření obrazů médií závisí na takových faktorech jako na množství volné paměti a rychlosti, jakou jsou soubory protokolu vytvořeny.

Obnova z obrazů médií

Správce front automaticky obnoví některé objekty ze svého obrazu média během spuštění správce front. Zotavuje frontu automaticky, pokud byla zahrnuta do transakce, která byla nekompletní, když správce front byl naposledy ukončen, a během restartu byl nalezen poškozený nebo poškozený.

Ostatní objekty je třeba obnovit ručně pomocí příkazu **rcrmqobj**, který přehraje záznamy v protokolu k opětovnému vytvoření objektu IBM MQ. Objekt je znovu vytvořen z jeho posledního obrazu nalezeného v protokolu, spolu se všemi příslušnými událostmi protokolu mezi časem, kdy byl obraz uložen, a časem, kdy byl vydán příkaz k vytvoření nového vydání. Je-li objekt IBM MQ poškozen, jediné platné akce, které lze provést, jsou buď pro její odstranění, nebo pro opětovné vytvoření této metody. Netrvalé zprávy nelze tímto způsobem obnovit.

Další podrobnosti o příkazu **rcrmqobj** naleznete v souboru [rcrmqobj](#).

Soubor protokolu, který obsahuje záznam o obnově médií a všechny následné soubory protokolu, musí být k dispozici v adresáři souborů protokolu při pokusu o obnovení médií objektu. Pokud požadovaný soubor nelze najít, je vydána zpráva AMQ6767 a operace zotavení média selže. Pokud nevezmete pravidelné média s obrazy objektů, které chcete znovu vytvořit, můžete mít nedostatečný prostor na disku pro uchování všech souborů protokolu potřebných pro opětovné vytvoření objektu.

Obnova poškozených objektů během spouštění

Pokud správce front zjistí poškozený objekt během spouštění, závisí akce na typu objektu a na tom, zda je správce front konfigurován tak, aby podporoval zotavení z médií.

Pokud je objekt správce front poškozen, správce front se nemůže spustit, pokud jej nemůže obnovit. Je-li správce front konfigurován s lineárním protokolem, a tak podporuje obnovu médií, produkt IBM MQ se automaticky pokusí znovu vytvořit objekt správce front z jeho obrazů médií. Pokud vybraná metoda protokolu nepodporuje zotavení média, můžete buď obnovit zálohu správce front, nebo odstranit správce front.

Pokud byly při zastavení správce front aktivní nějaké transakce, lokální fronty obsahující trvalé a nepotvrzené zprávy, které byly vloženy do těchto transakcí nebo se dostaly do těchto transakcí, jsou rovněž nezbytné ke spuštění správce front. Pokud se zjistí, že se některé z těchto lokálních front poškodí, a správce front podporuje obnovu médií, pokusí se je automaticky znovu vytvořit z jejich obrazů médií. Pokud některou z front nelze obnovit, nelze spustit příkaz IBM MQ.

Jsou-li během zpracování spuštění ve správci front, který nepodporuje obnovu médií, zjištěny jakékoliv poškozené lokální fronty obsahující nepotvrzené zprávy, fronty se označí jako poškozené a budou ignorovány nepotvrzené zprávy. Tato situace je, protože není možné provést obnovu médií poškozených objektů na takovém správci front a jediná akce, která zbývá, je odstranit je. Byla vydána zpráva AMQ7472, která hlásí jakoukoli škodu.

Obnova poškozených objektů v jiných časech

Obnova médií objektů je automatická pouze během spouštění. V jiných případech je při zjištění poškození objektu vydána zpráva operátora AMQ7472 a většina operací s použitím objektu se nezdaří. Je-li objekt správce front poškozen v libovolném okamžiku po spuštění správce front, provede správce front preventivní ukončení. Když je objekt poškozen, můžete jej vymazat nebo, pokud správce front používá lineární protokol, pokuste se jej obnovit z obrazu svých médií pomocí příkazu **rcrmqobj** (další podrobnosti viz [rcrmqobj](#)).

Zabezpečení souborů protokolu produktu IBM MQ

Nedotýkejte se souborů protokolu, když je správce front spuštěn, obnova může být nemožná. Použijte superuživatele nebo oprávnění mqm k ochraně souborů protokolu proti neúmyslné úpravě.

Neodebírejte aktivní soubory protokolu ručně, je-li spuštěn správce front produktu IBM MQ . Pokud uživatel neúmyslně odstraní soubory protokolu, které správce front potřebuje restartovat, produkt IBM MQ **neprovádí** žádné chyby a pokračuje v zpracování dat *včetně trvalých zpráv*. Správce front se normálně ukončí, ale nespustí se znovu. Navrácení zpráv se pak stane nemožným.

Uživatelé s oprávněním k odebírání protokolů, které jsou používány aktivním správcem front, mají také oprávnění k odstraňování jiných důležitých prostředků správce front (například souborů fronty, katalogu objektů a spustitelných souborů produktu IBM MQ). Mohou tedy poškodit běžící nebo nečinné správce front způsobem, který nedokáže ochránit sám IBM MQ .

Dávejte pozor při udělování superuživatele nebo oprávnění mqm.

Výpis obsahu protokolu pomocí příkazu dmpmqlog

Chcete-li vypsát obsah protokolu správce front, použijte příkaz dmpmqlog k výpisu obsahu protokolu správce front.

Chcete-li vypsát obsah protokolu správce front, použijte příkaz dmpmqlog . Standardně jsou všechny aktivní záznamy žurnálu vypsány, to znamená, že příkaz spouští výpis paměti z hlavičky protokolu (obvykle od začátku posledního dokončeného kontrolního bodu).

Protokol lze obvykle vypsát pouze v případě, že není spuštěn správce front. Vzhledem k tomu, že správce front přijímá kontrolní bod během ukončování práce, aktivní část protokolu obvykle obsahuje malý počet záznamů protokolu. Příkaz dmpmqlog však můžete použít k vypsání více záznamů protokolu pomocí jedné z následujících voleb, abyste změnili počáteční pozici výpisu:

- Spuštění výpisu paměti z *báze* protokolu. Základ protokolu je první záznam protokolu v souboru protokolu, který obsahuje hlavičku protokolu. Množství dalších dat vypsanych v tomto případě závisí na tom, kde se hlava protokolu nachází v souboru protokolu. Pokud se blíží ke začátku souboru protokolu, vypíše se pouze malý objem dalších dat. Pokud se hlava nachází v blízkosti konce souboru protokolu, bude vypsána podstatně více dat.
- Určete počáteční pozici výpisu paměti jako jednotlivý záznam protokolu. Každý záznam protokolu je identifikován jedinečným *pořadovým číslem protokolu (LSN)*. V případě kruhového protokolování nesmí tento záznam počátečního protokolu existovat před základní úrovni protokolu; toto omezení se nevztahuje na lineární protokoly. Možná budete muset obnovit neaktivní soubory protokolu před spuštěním příkazu. Je třeba určit platné pořadové číslo v protokolu přijaté od předchozího výstupu příkazu dmpmqlog jako počáteční pozice.

Například s lineárním protokolováním můžete zadat nextlsn ze svého posledního výstupu dmpmqlog . Hodnota nextlsn se zobrazí v parametru Log File Header a udává pořadové číslo v žurnálu dalšího záznamu protokolu, který má být zapsán. Použijte tuto pozici jako počáteční pozici pro formátování všech záznamů protokolu, které byly zapsány od posledního výpisu protokolu.

- **Pouze pro lineární protokoly** můžete instruovat dmpmqlog , aby se záznamy protokolu spustily z jakéhokoli rozsahu daného souboru protokolu. V tomto případě produkt dmpmqlog očekává, že najde tento soubor protokolu a každý po sobě jdoucí, ve stejném adresáři jako aktivní soubory protokolu. Tato volba se nevztahuje na kruhové protokoly, kde dmpmqlog nemůže získat přístup k záznamům protokolu před bázi protokolu.

Výstup z příkazu dmpmqlog je Log File Header a řada formátovaných záznamů protokolu. Správce front používá několik záznamů žurnálu k zaznamenání změn svých dat.

Některé z informací, které jsou formátovány, se používají pouze interně. Následující seznam obsahuje nejužitečnější záznamy protokolu:

Hlavička souboru žurnálu.

Každý protokol má jediné záhlaví souboru protokolu, které je vždy první věcí formátovanou příkazem dmpmqlog . Obsahuje následující pole:

<i>logactive</i>	Počet oblastí primárního protokolu.
<i>loginactive</i>	Počet sekundárních fyzických oblastí protokolu.
<i>velikost_protokolu</i>	Počet stránek o velikosti 4 kB za fyzickou oblast.
<i>základ_sn</i>	První LSN v rozsahu protokolu obsahující hlavu protokolu.
<i>nextlsn</i>	Pořadové číslo LSN dalšího záznamu protokolu, který má být zapsán.
<i>headlsn</i>	Pořadové číslo protokolu záznamu v protokolu v záhlaví protokolu.
<i>tailsn</i>	Pořadové číslo v protokolu LSN označující koncovou pozici protokolu v protokolu.
<i>hflag1</i>	Zda se jedná o protokol CIRCULAR nebo LOG RETAIN (lineární).
<i>IDHeadExtentID</i>	Oblast protokolu obsahující hlavičku protokolu.

Záhlaví záznamu protokolu

Každý záznam protokolu v rámci protokolu má pevné záhlaví obsahující následující informace:

<i>LSN</i>	Pořadové číslo v protokolu.
<i>LogRecdTyp</i>	Typ záznamu protokolu.
<i>XTrand</i>	Identifikátor transakce přidružený k tomuto záznamu protokolu (pokud existuje). <i>TranType</i> rozhraní MQI označuje pouze transakci typu IBM MQ-only. <i>TranType</i> z XA se podílí na jiných správcích prostředků. Aktualizace zahrnuté do stejné jednotky práce mají stejný <i>XTranid</i> .
<i>QueueName</i>	Fronta přidružená k tomuto záznamu protokolu (pokud existuje).
<i>Qid</i>	Jedinečný vnitřní identifikátor fronty.
<i>PrevLSN</i>	Pořadové číslo předchozího záznamu protokolu v protokolu v rámci stejné transakce (je-li k tomu došlo).

Spustit správce front

Protokoly, které správce front spustil.

<i>StartDate</i>	Datum, kdy byl spuštěn správce front.
<i>StartTime</i>	Čas, kdy byl správce front spuštěn.

Zastavit správce front

Protokoly, které správce front zastavily.

<i>StopDate</i>	Datum, kdy byl zastaven správce front.
<i>StopTime</i>	Čas zastavení správce front.
<i>ForceFlag</i>	Typ použitého ukončení práce.

Začátek kontrolního bodu

To označuje začátek kontrolního bodu správce front.

Koncový kontrolní bod

To označuje konec kontrolního bodu správce front.

<i>ChkPtLSN</i>	Pořadové číslo v protokolu pro záznam protokolu, který spustil tento kontrolní bod.
-----------------	---

Vložit zprávu

Tím se protokolují trvalá zpráva do fronty. Pokud byla zpráva vložena pod synchronizační bod, záhlaví záznamu protokolu obsahuje nenull *XTranid*. Zbytek záznamu obsahuje:

<i>MapIndex</i>	Identifikátor pro zprávu ve frontě. Lze ji použít k porovnání odpovídajícího souboru MQGET , který byl použit k získání této zprávy z fronty. V tomto případě může být nalezen následný záznam protokolu <i>Get Message</i> obsahující stejné <i>QueueName</i> a <i>MapIndex</i> . V tomto okamžiku lze identifikátor <i>MapIndex</i> znovu použít pro následné vložení zprávy do této fronty.
<i>Data</i>	Obsaženo v hexadecimálním výpisu paměti pro tento záznam protokolu je různá vnitřní data následovaná reprezentací deskriptoru zpráv (eyecatcher MD) a pak samotná data zprávy.

Vložit část

Trvalé zprávy, které jsou příliš velké pro jeden záznam protokolu, se protokolují jako více záznamů protokolu *Put Part* následovaných jediným záznamem *Put Message* . Pokud existují záznamy *Put Part* , pak pole *PrevLSN* bude zřetěžit záznamy *Put Part* a konečný záznam *Put Message* dohromady.

<i>Data</i>	Pokračuje v datech zprávy tam, kde byl předchozí záznam protokolu ponechán mimo.
-------------	--

Získat zprávu

Protokolovány jsou pouze přístupy trvalých zpráv. Pokud se zpráva dostala pod synchronizační bod, záhlaví záznamu protokolu obsahuje non-null *XTranid*. Zbytek záznamu obsahuje:

<i>MapIndex</i>	Identifikuje zprávu, která byla načtena z fronty. Nejnovější záznam protokolu <i>Put Message</i> obsahující stejné <i>QueueName</i> a <i>MapIndex</i> identifikuje zprávu, která byla načtena.
<i>QPriority</i>	Priorita zprávy načtené z fronty.

Spustit transakci

Označuje začátek nové transakce. *TranType* rozhraní MQI označuje pouze transakci typu IBM MQ. *TranType XA* označuje název, který zahrnuje další správce prostředků. Všechny aktualizace provedené touto transakcí budou mít stejné *XTranid*.

Připravit transakci

Označuje, že správce front je připraven potvrdit aktualizace přidružené k zadanému *XTranid*. Tento záznam protokolu je zapsán jako součást dvoufázového potvrzování zahrnujícího ostatní správce prostředků.

Potvrdit transakci

Označuje, že správce front provedl potvrzení všech aktualizací provedených transakcí.

Odvolat transakci

To označuje záměr správce front odvolat transakci.

Ukončit transakci

To označuje konec odvolané transakce.

Tabulka transakcí

Tento záznam je zapsán během synchronizačního bodu. Zaznamená stav každé transakce, která provedla trvalé aktualizace. Pro každou transakci jsou zaznamenány následující informace:

<i>XTrand</i>	Identifikátor transakce.
<i>FirstLSN</i>	Pořadové číslo v protokolu prvního záznamu protokolu přidruženého k transakci.
<i>LastLSN</i>	Pořadové číslo v protokolu posledního záznamu protokolu přidruženého k transakci.

Účastníci transakce

Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Záznamy o externích správcích prostředků, kteří se účastní transakcí. Pro každého účastníka se zaznamená následující:

<i>RMName</i>	Název správce prostředků.
<i>RMID</i>	Identifikátor správce prostředků. To je také zaprotokolováno v následných záznamech protokolu <i>Transaction Prepared</i> , které zaznamenávají globální transakce, v nichž se správce prostředků podílí.
<i>SwitchFile</i>	Soubor načtení přepínače pro tohoto správce prostředků.
<i>XAOpenString</i>	Otevřený řetězec XA pro tohoto správce prostředků.
<i>XACloseString</i>	Řetězec zavření XA pro tohoto správce prostředků.

Připravená transakce

Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Označuje, že zadaná globální transakce byla úspěšně připravena. Každý zúčastněný správce prostředků bude instruován k potvrzení. *RMID* každého připraveného správce prostředků je zaznamenáno v záznamu protokolu. Účastní-li se správce front v transakci *Participant Entry* s hodnotou *RMID*, bude přítomna hodnota nula.

Zapomenutí transakce

Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Je-li rozhodnutí o potvrzení přijato každému účastníkovi, následuje záznam protokolu produktu *Transaction Prepared*.

Vyprázdnit frontu

Tím se protokolují informace o tom, že všechny zprávy ve frontě byly vyprázdněny, například pomocí příkazu MQSC CLEAR QUEUE.

Atributy fronty

Tím se protokolují inicializace nebo změna atributů fronty.

Vytvořit objekt

Tím se protokolují vytvoření objektu IBM MQ.

<i>ObjName</i>	Název objektu, který byl vytvořen.
<i>UserId</i>	ID uživatele, který provádí vytvoření.

Odstranit objekt

Tím se protokolují odstranění objektu IBM MQ.

<i>ObjName</i>	Název objektu, který byl odstraněn.
----------------	-------------------------------------

Zálohování a obnova dat správce front produktu IBM MQ

Zálohování správců front a dat správce front.

Periodicky můžete přijmout opatření k ochraně správců front proti možnému poškození způsobenému hardwarovými poruchami. Existují tři způsoby ochrany správce front:

Zálohovat data správce front

Dojde-li k selhání hardwaru, může být vynucen jeho zastavení správce front. Dojde-li ke ztrátě dat protokolu správce front v důsledku selhání hardwaru, může být správce front schopen restartovat. Pokud zálohujete data správce front, můžete být schopni obnovit některé nebo všechny údaje o ztracených datech správce front.

Obecně platí, že čím častěji zálohujete data správce front, tím méně dat ztratíte v případě selhání hardwaru, které vede ke ztrátě integrity protokolu pro zotavení.

Chcete-li zálohovat data správce front, nesmí být správce front spuštěn.

Chcete-li zálohovat a obnovit data správce front, prohlédněte si:

- [“Zálohování dat správce front”](#) na stránce 476.
- [“Obnova dat správce front”](#) na stránce 477.

Použit správce front zálohování

Je-li selhání hardwaru závažné, může být správce front nezotavitelný. V této situaci může být správce front zálohy aktivován v případě neodstranitelného správce front, pokud má správce front nezotavitelné správce front vyhrazené záložní správce front. Pokud byl aktualizován pravidelně, může protokol správce front zálohy obsahovat data protokolu, která obsahují poslední dokončený protokol ze nezotavitelného správce front.

Záložní správce front může být aktualizován v době, kdy je stále spuštěn existující správce front.

Chcete-li vytvořit a aktivovat záložní správce front, postupujte podle následujících kroků:

- [“Vytvoření správce front zálohování”](#) na stránce 478.
- [“Spuštění záložního správce front”](#) na stránce 479.

Zálohovat pouze konfiguraci správce front

Dojde-li k selhání hardwaru, může být vynucen jeho zastavení správce front. Dojde-li ke ztrátě konfigurace správce front i dat protokolu v důsledku selhání hardwaru, nebude možné správce front restartovat nebo jej obnovit z protokolu. Pokud zálohujete konfiguraci správce front, bylo by možné znovu vytvořit správce front a všechny jeho objekty z uložených definic.

Chcete-li zálohovat konfiguraci správce front, musí být spuštěn správce front.

Chcete-li zálohovat a obnovit konfiguraci správce front, přečtěte si následující informace:

- [“Zálohování konfigurace správce front”](#) na stránce 480
- [“Obnovení konfigurace správce front”](#) na stránce 480

Zálohování dat správce front

Zálohování dat správce front vám může pomoci chránit před možnou ztrátou dat způsobenou hardwarovými chybami.

Než začnete

Ujistěte se, že správce front není spuštěn. Pokud se pokusíte provést zálohu spuštěného správce front, záloha nemusí být konzistentní, protože při kopírování souborů došlo k jeho aktualizacím. Je-li to možné, zastavte správce front spuštěním příkazu `endmqm -w` (ukončení čekání), pouze pokud selže, použijte příkaz `endmqm -i` (okamžité ukončení činnosti systému).

Informace o této úloze

Chcete-li vytvořit záložní kopii dat správce front, proveďte následující úlohy:

1. Vyhledejte adresáře, pod kterými správce front umísťuje svá data a soubory protokolu za použití informací v konfiguračních souborech. Další informace viz [“Změna konfiguračních informací IBM MQ a správce front”](#) na stránce 81.

Poznámka: Názvy, které se v adresáři objeví, se transformují, aby se zajistilo, že jsou kompatibilní s platformou, na které používáte produkt IBM MQ. Další informace o transformacích názvů najdete v tématu [Základní informace o názvech souborů produktu IBM MQ](#).

2. Převedte kopie všech dat správce front a adresářů souborů protokolu, včetně všech podadresářů.

Ujistěte se, že nechybí žádné soubory, zejména řídicí soubor protokolu, jak je popsáno v části [“Jaké protokoly vypadají jako”](#) na stránce 457, a konfigurační soubory, jak je popsáno v tématu [“Inicializační a konfigurační soubory”](#) na stránce 169. Některé adresáře mohou být prázdné, ale vy je budete potřebovat k obnovení zálohy později.

3. Zachovejte vlastnictví souborů. Pro systémy IBM MQ for UNIX a Linux to můžete provést pomocí příkazu `tar`. (Máte-li fronty větší než 2 GB, nelze použít příkaz `tar`. Další informace naleznete v tématu [Povolení velkých front](#).)

Poznámka: Provedete-li upgrade na produkt IBM WebSphere MQ 7.5 a později, ujistěte se, že jste provedli zálohu souboru `.ini` a položek registru. Informace o správci front jsou uloženy v souboru `.ini` a lze je použít k vrácení zpět na předchozí verzi produktu IBM MQ.

Obnova dat správce front

Chcete-li obnovit zálohu dat správce front, postupujte podle následujících kroků.

Než začnete

Ujistěte se, že správce front není spuštěn.

Když obnovujete zálohu správce front v klastru, prohlédněte si téma [“Obnova správce front klastru”](#) na stránce 291 a [Klastrování: Availability, multi-instance a disaster recovery](#), kde získáte další informace.

Informace o této úloze

Chcete-li obnovit zálohu dat správce front, postupujte takto:

1. Pomocí informací v konfiguračních souborech vyhledejte adresáře, pod kterými správce front umísťuje svá data a příslušné soubory protokolu.
2. Vyprázdněte adresáře, do kterých chcete umístit data typu "backedup".
3. Zkopírujte data správce front-up a soubory protokolu do správných míst.
4. Aktualizujte soubory s informacemi o konfiguraci.

Zkontrolujte výslednou adresářovou strukturu a ujistěte se, že máte všechny požadované adresáře.

Další informace o adresářích a podadresářích produktu IBM MQ viz [Adresářová struktura v systémech Windows](#) a [Obsah adresáře v systémech SYSTÉM UNIX a Linux](#).

Ujistěte se, že máte soubor s řízením protokolu a také soubory protokolu. Také zkontrolujte, zda jsou konfigurační soubory IBM MQ a správce front konzistentní, takže produkt IBM MQ může vyhledávat obnovená data na správných místech.

Pro kruhové protokolování zálohujte data správce front a adresáře souborů protokolu ve stejnou dobu, abyste mohli obnovit konzistentní sadu dat a protokolů správce front.

V případě lineární protokolování zálohujte data správce front a adresáře souborů protokolu současně. Je-li k dispozici odpovídající úplná posloupnost souborů žurnálu, je možné obnovit pouze datové soubory správce front.

Poznámka: Provedete-li upgrade na produkt IBM WebSphere MQ 7.5 a později, ujistěte se, že jste provedli zálohu souboru `.ini` a položek registru. Informace o správci front jsou uloženy v souboru `.ini` a lze je použít k vrácení zpět na předchozí verzi produktu IBM MQ.

Výsledky

Pokud byla data zálohována a obnovena správně, bude správce front nyní spuštěn.

Použití správce front zálohování

Existující správce front může mít vyhrazeného správce front zálohování.

Záložní správce front je neaktivní kopie existujícího správce front. Pokud se stávající správce front stane neobnovitelným kvůli závažnému selhání hardwaru, lze správce front zálohy převést do režimu online a nahradit neodstranitelného správce front.

Existující soubory protokolu správce front musí být pravidelně kopírovány do správce front zálohování, aby bylo zajištěno, že správce front zálohování zůstane účinnou metodou pro zotavení z havárie. Existující

správce front není třeba zastavit pro soubory žurnálu, které mají být zkopírovány, avšak pouze v případě, že správce front dokončil zápis do protokolu, je třeba zkopírovat pouze soubor protokolu. Protože se existující protokol správce front průběžně aktualizuje, je mezi stávajícím protokolem správce front a daty protokolu zkopírovanými do protokolu správce front pro zálohování zkopírováno nepatrné rozdíly mezi existujícím protokolem správce front a daty protokolu. Pravidelné aktualizace správce front zálohování minimalizuje rozdíly mezi dvěma protokoly.

Je-li nutné správce front zálohování převést do režimu online, musí být aktivován a poté spuštěn. Požadavek na aktivaci správce front zálohy předtím, než je spuštěn, je preventivní opatření, které má být chráněno proti náhodnému spuštění zálohovacího správce front. Poté, co je správce front zálohování aktivován, již jej nelze aktualizovat.

Informace o tom, jak vytvořit, aktualizovat a spustit správce front zálohování, najdete v následujících tématech:

- [“Vytvoření správce front zálohování” na stránce 478](#)
- [“Aktualizace záložního správce front” na stránce 478](#)
- [“Spuštění záložního správce front” na stránce 479](#)

Vytvoření správce front zálohování

Při použití lineárního protokolování můžete použít pouze správce front zálohování.

Chcete-li vytvořit správce front zálohování pro existujícího správce front, postupujte takto:

1. Vytvořte správce front zálohy pro existujícího správce front pomocí příkazu ovládacího prvku `STMQM`. Záložní správce front vyžaduje následující:
 - Chcete-li mít stejné atributy jako existující správce front, například název správce front, typ protokolování a velikost souboru protokolu.
 - Má být na stejné platformě jako existující správce front.
 - Být na stejné nebo vyšší úrovni kódu, než je úroveň kódu existující správce front.
2. Převeďte kopie všech existujících dat správce front a adresářů souborů protokolu, včetně všech podadresářů, jak je popsáno v tématu [“Zálohování dat správce front” na stránce 476](#).
3. Přepište soubory dat a adresáře souborů správce front zálohování, včetně všech podadresářů, s kopiemi převzatovými z existujícího správce front.
4. Proveďte následující řídicí příkaz na správci front zálohování:

```
stmqm -i BackupQMName
```

Tento příkaz označí správce front jako správce front zálohy v rámci produktu IBM MQa přehraje všechny zkopírované oblasti protokolu k převedení správce front zálohy v kroku s existujícím správcem front.

Aktualizace záložního správce front

Chcete-li zajistit, aby záložní správce front zůstal účinnou metodou pro zotavení z havárie, musí být pravidelně aktualizován.

Pravidelná aktualizace snižuje rozdíly mezi záložním protokolem správce front protokolu a aktuálním protokolem správce front. Není třeba zastavovat správce front, aby byl zálohován.

Chcete-li aktualizovat správce front zálohování, postupujte takto:

1. Na správce front, který má být zálohován, zadejte následující příkaz skriptu (MQSC):

```
RESET QMGR TYPE(ADVANCELOG)
```

Tím dojde k zastavení libovolného zápisu do aktuálního protokolu a následné zálohy protokolování správce front do dalšího rozsahu protokolu. Tím je zajištěno, že zálohujete všechny informace zaprotokolované do aktuálního času.

2. Získejte (nové) aktuální číslo fyzické oblasti aktivního protokolu zadáním následujícího příkazu skriptu (MQSC) na správci front, který má být zálohován:

```
DIS QMSTATUS CURRLOG
```

3. Zkopírujte aktualizované soubory rozsahu protokolu z aktuálního adresáře protokolu správce front do adresáře protokolu správce front zálohy-zkopírujte všechny oblasti pro rozšíření protokolu od poslední aktualizace a až po (nikoli však včetně) aktuální fyzické oblasti uvedené v kroku 2. Kopírovat pouze soubory rozsahu protokolu, ty začínající znaky "S. ..".
4. Na záložním správci front zadejte následující řídicí příkaz:

```
stmqm -i BackupQMName
```

Tím přehraje všechny kopírované oblasti protokolu a převede správce front do kroku se správcem front. Jakmile se přehrávání dokončí, obdržíte zprávu, která identifikuje všechny oblasti, které jsou nezbytné pro obnovu restartu, a všechny oblasti, které jsou nezbytné pro obnovení médií.

Varování: Kopírujete-li sadu protokolů non-contiguous do adresáře protokolu správce front zálohy, budou přehrány pouze protokoly, které jsou až do bodu, kde je nalezen první chybějící protokol.

Spuštění záložního správce front

Záložní správce front můžete nahradit nezotavitelným správcem front.

Chcete-li to provést, proveďte následující kroky:

1. Chcete-li aktivovat správce front pro zálohování, proveďte následující řídicí příkaz:

```
stmqm -a BackupQMName
```

Záložní správce front je aktivován. Aktivní správce front zálohy již nelze aktualizovat.

2. Spuštěním následujícího příkazu ovládacího prvku spusťte správce front zálohování:

```
stmqm BackupQMName
```

IBM MQ považuje toto zotavení za opětovné spuštění a využívá protokol ze správce front zálohování. Během poslední aktualizace pro přehrávání správce front zálohování se bude vyskytnout pouze aktivní transakce z naposledy zaznamenaného kontrolního bodu.

Je-li správce front zálohování nahrazen neobnovitelným správcem front, může dojít ke ztrátě dat správce front z neobnovitelného správce front. Množství ztracených dat závisí na tom, jak nedávno byl správce front zálohování naposledy aktualizován. Čím novější je poslední aktualizace, tím menší ztráta dat správce front.

3. Restartujte všechny kanály.

Zkontrolujte výslednou adresářovou strukturu a ujistěte se, že máte všechny požadované adresáře.

Další informace o adresářích a podadresářích produktu IBM MQ najdete v tématu [Plánování podpory systému souborů](#).

Ujistěte se, že máte soubor s řízením protokolu a také soubory protokolu. Také zkontrolujte, zda jsou konfigurační soubory produktu IBM MQ a správce front konzistentní, aby se produkt IBM MQ mohl podívat na správná místa obnovených dat.

Pokud byla data zálohována a obnovena správně, bude správce front nyní spuštěn.

Poznámka: I když jsou data správce front a soubory protokolu uloženy v různých adresářích, zálohují a obnovují adresáře ve stejnou dobu. Pokud se data a soubory protokolu správce front liší od stáří, správce front se nenachází v platném stavu a pravděpodobně nebude spuštěn. Pokud se spustí, vaše data budou pravděpodobně poškozena.


Zálohování konfigurace správce front

Zálohování konfigurace správce front vám může pomoci s novým sestavením správce front z jeho definic.

Chcete-li vytvořit záložní kopii konfigurace správce front, postupujte takto:

1. Zkontrolujte, zda je správce front spuštěn.
2. a. U příkazů AIX, HP-UX, Linux, Solarisnebo Windows: spusťte příkaz MQ Configuration (dmpmqcfg) pomocí výchozí volby formátování MQSC (-f mqsc) MQSC a všech atributů (-a), použijte přesměrování standardního výstupu pro ukládání definic do souboru, například:

```
dmpmqcfg -m MYQMGR -a > /mq/backups/MYQMGR.mqsc
```

- b.  V produktu IBM i: spusťte příkaz Výpis paměti MQ (DMPMQMCFG) pomocí výchozí volby formátování OUTPUT (*MQSC) a EXPATTR (*ALL), použijte soubory TOFILE a TOMBR k uložení definic do členu fyzického souboru, například:




```
DMPMQMCFG MQMNAME(MYQMGR) OUTPUT(*MQSC) EXPATTR(*ALL) TOFILE(QMQMSAMP/QMQSC)  
TOMBR(MYQMGRDEF)
```

Obnovení konfigurace správce front


Chcete-li obnovit zálohu konfigurace správce front, postupujte podle následujících kroků.

Chcete-li obnovit zálohu konfigurace správce front, postupujte takto:

1. Zkontrolujte, zda je správce front spuštěn. Všimněte si, že správce front mohl být znovu vytvořen, pokud je poškození dat a protokolů neopravitelné jinými prostředky.
2. V závislosti na platformě proveďte jeden z následujících příkazů:

- a.    V systémech AIX, HP-UX, Linux, Solarisnebo Windows: Provést **runmqsc** proti správci front použijte standardní přesměrování vstupu pro obnovení definic ze souboru skriptu generovaného příkazem MQ Configuration (**dmpmqcfg**), například:

```
runmqsc MYQMGR < /mq/backups/MYQMGR.mqsc
```

- b.  V produktu IBM i: Provést **STRMQMMQSC** proti správci front použijte příkaz **SRCMBR** a **SRCFILE** k obnovení definic z členu fyzického souboru generovaného příkazem MQ pro výpis paměti (**DMPMQMCFG**), například:

```
STRMQMMQSC MQMNAME(MYQMGR) SRCFILE(QMQMSAMP/QMQSC) SRCMBR(MYQMGR)
```

Související informace

[dmpmqcfg \(konfigurace správce front výpisu\)](#)

Konfigurace prostředků produktu JMS

Jedním z způsobů, jak může aplikace produktu JMS vytvořit a konfigurovat prostředky, které potřebuje pro připojení k produktu IBM MQ a k místům určení pro odesílání nebo příjem zpráv, je pomocí rozhraní JNDI (Java Naming and Directory Interface) načítat spravované objekty z umístění v rámci služby pro správu pojmenování a adresářů, která se nazývá obor názvů JNDI. Než bude moci aplikace JMS načíst spravované objekty z oboru názvů JNDI, musíte nejprve vytvořit a nakonfigurovat spravované objekty.

Informace o této úloze

Spravované objekty v produktu IBM MQ můžete vytvářet a konfigurovat pomocí jednoho z následujících nástrojů:

MQ Explorer

Pomocí produktu MQ Explorer můžete vytvářet a spravovat definice objektů produktu JMS, které jsou uloženy v LDAP, v lokálním systému souborů nebo v jiných umístěních.

Administrační nástroj produktu IBM MQ JMS

Administrativní nástroj produktu IBM MQ JMS je nástroj příkazového řádku, který můžete použít k vytvoření a konfiguraci objektů produktu IBM MQ JMS uložených v LDAP, v lokálním systému souborů nebo v jiných umístěních. Administrativní nástroj produktu JMS používá syntaxi podobnou produktu **runmqsc** také podporuje skriptování.

Nástroj pro správu používá konfigurační soubor k nastavení hodnot určitých vlastností. K dispozici je ukázkový konfigurační soubor, který můžete upravit tak, aby vyhovoval vašemu systému, než začnete používat nástroj ke konfiguraci prostředků produktu JMS. Další informace o konfiguračním souboru viz téma [“Konfigurace nástroje pro administraci produktu JMS”](#) na stránce 487.

Aplikace produktu IBM MQ JMS, které jsou implementovány do produktu WebSphere Application Server, potřebují přistupovat k objektům produktu JMS z úložiště JNDI aplikačního serveru. Proto pokud používáte systém zpráv produktu JMS mezi WebSphere Application Server a IBM MQ, musíte vytvořit objekty v WebSphere Application Server, které odpovídají objektům, které vytvoříte v produktu IBM MQ.

MQ Explorer a administrační nástroj produktu IBM MQ JMS nelze použít ke správě objektů produktu IBM MQ JMS uložených v produktu WebSphere Application Server. Místo toho můžete vytvořit a konfigurovat spravované objekty v produktu WebSphere Application Server pomocí jednoho z následujících nástrojů:

WebSphere Application Server Administrativní konzola

Administrativní konzola produktu WebSphere Application Server je webový nástroj, který lze použít ke správě objektů produktu IBM MQ JMS v produktu WebSphere Application Server.

WebSphere Application Server skriptovací klient wsadmin

Skriptovací klient wsadmin produktu WebSphere Application Server poskytuje specializované příkazy pro správu objektů produktu IBM MQ JMS v produktu WebSphere Application Server.

Chcete-li použít aplikaci JMS pro přístup k prostředkům správce front produktu IBM MQ z produktu WebSphere Application Server, musíte použít poskytovatele systému zpráv produktu IBM MQ v produktu WebSphere Application Server, který obsahuje verzi produktu IBM MQ classes for JMS. Adaptér prostředků produktu IBM MQ, který je dodáván s produktem WebSphere Application Server, používají všechny aplikace, které provozují systém zpráv produktu JMS s poskytovatelem systému zpráv produktu IBM MQ. Adaptér prostředků produktu IBM MQ se obvykle aktualizuje automaticky při použití opravných sad WebSphere Application Server, ale pokud jste již dříve ručně aktualizovali adaptér prostředků, musíte ručně aktualizovat konfiguraci, abyste se ujistili, že je údržba správně aplikována.

Související informace

[Zápis aplikací IBM MQ classes for JMS](#)
[runmqsc](#)

Konfigurace továren připojení a míst určení v oboru názvů JNDI

Aplikace produktu JMS přistupují ke spravovaným objektům v rámci služby pro správu pojmenování a adresářů prostřednictvím rozhraní JNDI (Java Naming and Directory Interface). Spravované objekty produktu JMS jsou uloženy v umístění v rámci služby pro správu pojmenování a adresářů, na které se odkazuje jako na obor názvů JNDI. Aplikace JMS může vyhledat spravované objekty a připojit se k IBM MQ a přistupovat k místům určení pro odesílání nebo příjem zpráv.

Informace o této úloze

Aplikace produktu JMS vyhledají názvy objektů produktu JMS ve službě pro správu pojmenování a adresářů s použitím kontextů:

počáteční kontext

Počáteční kontext definuje kořen oboru názvů JNDI. Pro každé umístění ve službě pro správu pojmenování a adresářů musíte zadat počáteční kontext, ze kterého uvedete počáteční bod, ze kterého může aplikace JMS vyřešit názvy spravovaných objektů v tomto umístění služby pro pojmenování a adresářovou službu.

Dílčí kontexty

Kontext může mít jeden nebo více dílčích kontextů. Dílčí kontext je dílčím oddílem oboru názvů JNDI a může obsahovat spravované objekty, jako jsou továrny připojení a místa určení, stejně jako další dílčí kontexty. Dílčí kontext není sám o sobě objektem. Je pouze rozšířením konvence pojmenování objektů v dílčím kontextu.

Kontexty můžete vytvořit buď pomocí produktu MQ Explorer , nebo pomocí nástroje pro administraci produktu IBM MQ JMS .

Než bude moci aplikace IBM MQ classes for JMS načíst spravované objekty z oboru názvů JNDI, musíte nejprve vytvořit spravované objekty buď pomocí produktu MQ Explorer , nebo pomocí nástroje pro administraci produktu IBM MQ JMS . Můžete vytvářet a konfigurovat následující typy objektů produktu JMS :

Továrna připojení

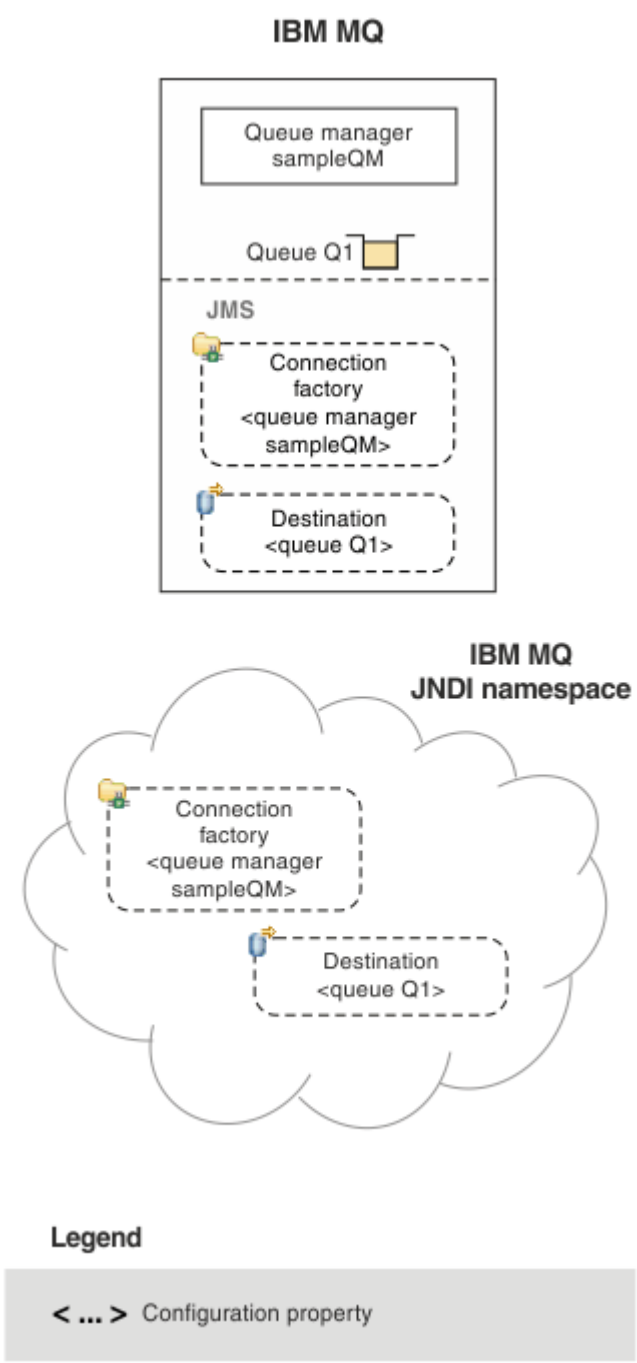
Objekt továrny připojení produktu JMS definuje sadu standardních vlastností konfigurace pro připojení. Aplikace JMS používá továrnu připojení k vytvoření připojení k produktu IBM MQ. Můžete vytvořit továrnu připojení, která je specifická pro jednu z těchto domén systému zpráv, doménu systému zpráv typu point-to-point a doménu systému zpráv publikování/odběru. Volitelně můžete z produktu JMS 1.1 vytvořit továrny připojení nezávislé na doméně, které lze použít pro systém zpráv typu point-to-point i publikování/odběr.

Místo určení

Místo určení JMS je objekt, který představuje cíl zpráv, které klient produkuje, a zdroj zpráv, které aplikace JMS přijímá. Aplikace JMS může buď použít jediný cílový objekt pro vkládání zpráv a získání zpráv od nich, nebo může aplikace používat samostatné cílové objekty. Existují dva typy cílového objektu:

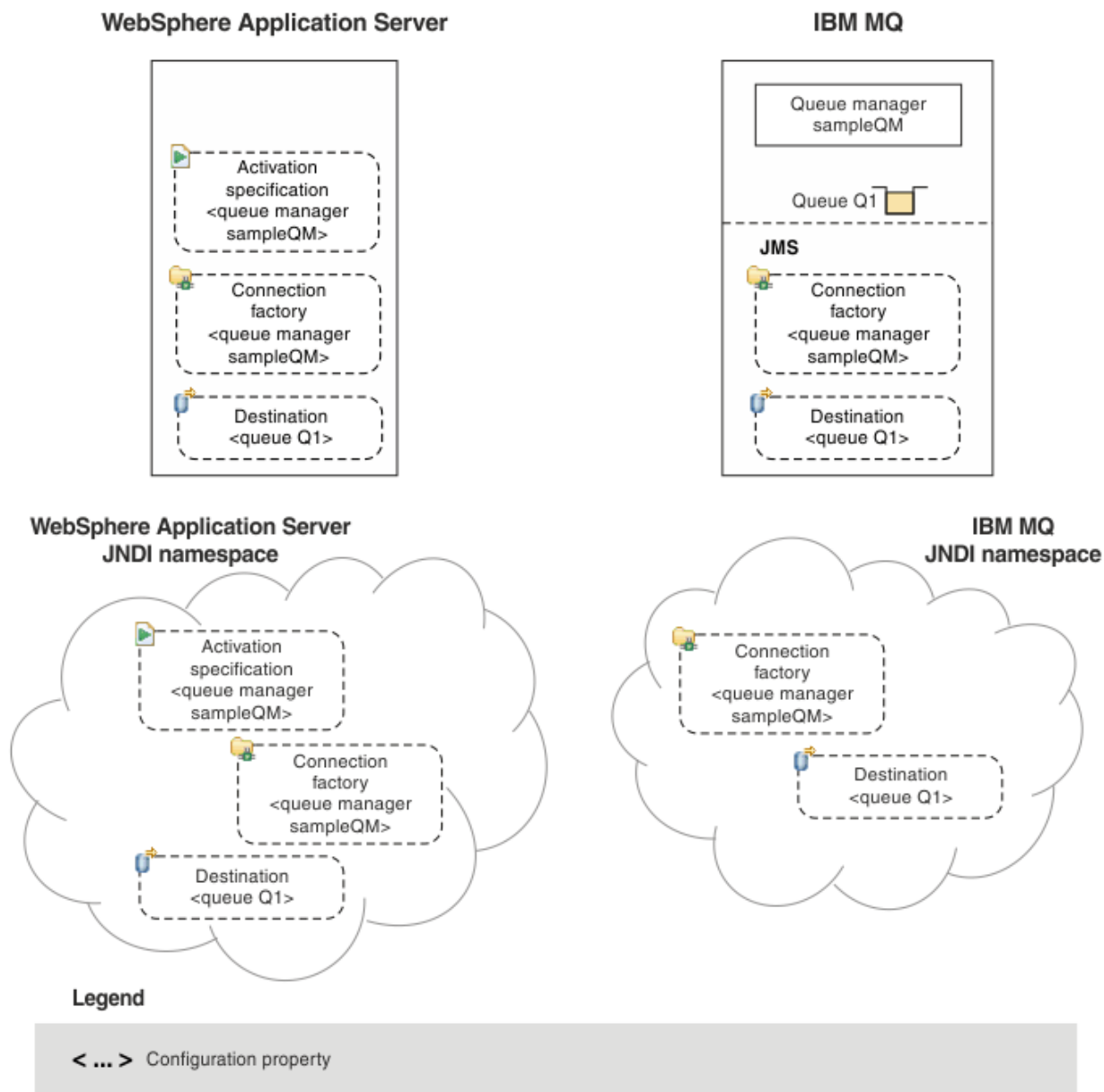
- Místo určení fronty JMS použité v dvoubodovém systému zpráv
- Místo určení tématu JMS použité v systému zpráv publikování/odběru

Následující diagram ukazuje příklad objektů produktu JMS vytvořených v oboru názvů JNDI produktu IBM MQ .



Obrázek 82. Objekty JMS vytvořené v produktu IBM MQ

Pokud používáte systém zpráv produktu JMS mezi produkty WebSphere Application Server a IBM MQ, musíte vytvořit odpovídající objekty v produktu WebSphere Application Server, které budou použity ke komunikaci s produktem IBM MQ. Při vytváření jednoho z těchto objektů v produktu WebSphere Application Server je tento objekt uložen v oboru názvů rozhraní JNDI produktu WebSphere Application Server, jak je uvedeno v následujícím diagramu.



Obrázek 83. Objekty vytvořené v produktu WebSphere Application Servera odpovídající objekty v produktu IBM MQ

Pokud vaše aplikace používá objekt MDB (Message-driven bean), bude továrna připojení použita pouze pro odchozí zprávy a příchozí zprávy jsou přijímány specifikací aktivace. Specifikace aktivace jsou součástí standardu Java EE Connector Architecture 1.5 (JCA 1.5). Produkt JCA 1.5 poskytuje standardní způsob integrace poskytovatelů produktu JMS, jako je například produkt IBM MQ, s aplikačními servery Java EE, jako je například produkt WebSphere Application Server. Specifikace aktivace JMS může být přidružena k jednomu nebo více objektům typu message-driven bean (MDB) a poskytuje konfiguraci nezbytnou pro příjem těchto objektů MDB pro zprávy přicházející do místa určení.

K vytvoření a konfiguraci prostředků produktu JMS, které potřebujete, můžete použít buď administrativní konzolu produktu WebSphere Application Server, nebo skriptovací příkazy wsadmin.

Procedura

- Chcete-li nakonfigurovat objekty produktu JMS pro prostor IBM MQ pomocí produktu MQ Explorer, viz ["Konfigurace objektů produktu JMS pomocí produktu MQ Explorer"](#) na stránce 485.

- Chcete-li nakonfigurovat objekty produktu JMS pro prostor IBM MQ pomocí nástroje pro administraci produktu IBM MQ JMS , přečtěte si téma [“Konfigurace objektů produktu JMS pomocí nástroje pro administraci”](#) na stránce 486.
- Chcete-li konfigurovat objekty JMS pro produkt WebSphere Application Server, viz [“Konfigurace prostředků produktu JMS v produktu WebSphere Application Server”](#) na stránce 495.

Výsledky

Aplikace produktu IBM MQ classes for JMS může načíst spravované objekty z oboru názvů rozhraní JNDI a v případě potřeby nastavit nebo změnit jednu či více vlastností pomocí rozšíření produktu IBM JMS nebo rozšíření produktu IBM MQ JMS .

Související informace

[Použití JNDI k načtení spravovaných objektů v aplikaci JMS](#)

[Vytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS](#)

Konfigurace objektů produktu JMS pomocí produktu MQ Explorer

Pomocí grafického uživatelského rozhraní produktu MQ Explorer vytvořte objekty produktu JMS z objektů IBM MQ a objekty IBM MQ z objektů JMS a také pro administraci a monitorování dalších objektů produktu IBM MQ .

Informace o této úloze

MQ Explorer je grafické uživatelské rozhraní, ve kterém můžete spravovat a monitorovat objekty IBM MQ, ať je jejich hostitelem lokální počítač nebo vzdálený systém. Produkt MQ Explorer lze provozovat v systémech Windows a Linux x86-64. Může se vzdáleně připojovat ke správcům front spuštěným na jakékoli podporované platformě včetně produktu z/OS, a umožnit tak zobrazení, prozkoumání a pozměňování celé komunikační páteře systému zpráv z konzoly.

V produktu MQ Explorer jsou všechny továrny připojení uloženy ve složkách Továrny připojení v příslušném kontextu a dílčích kontextech.

Můžete provádět následující typy úloh s produktem MQ Explorer, buď kontextově z existujícího objektu v produktu MQ Explorer, nebo v rámci průvodce vytvořením nového objektu:

- Vytvořte továrnu připojení produktu JMS z libovolného z následujících objektů produktu IBM MQ :
 - Správce front produktu IBM MQ , ať už na lokálním počítači nebo na vzdáleném systému.
 - Kanál IBM MQ .
 - Modul listener produktu IBM MQ .
- Přidejte správce front IBM MQ do produktu MQ Explorer pomocí továrny připojení produktu JMS .
- Vytvořte frontu JMS z fronty IBM MQ .
- Vytvořte frontu IBM MQ z fronty JMS .
- Vytvoření tématu JMS z tématu IBM MQ , které může být objektem IBM MQ nebo dynamickým tématem.
- Vytvoření tématu IBM MQ z tématu JMS .

Procedura

- Spusťte produkt MQ Explorer, pokud již není spuštěn.
Je-li produkt MQ Explorer spuštěn a zobrazí úvodní stránku, zavřete úvodní stránku a spusťte administraci objektů produktu IBM MQ .
- Pokud jste tak dosud neučinili, vytvořte počáteční kontext definující kořenový adresář oboru názvů JNDI, ve kterém jsou objekty JMS uloženy ve službě pro správu pojmenování a adresářů.
Po přidání počátečního kontextu do produktu MQ Explorer můžete v oboru názvů JNDI vytvořit objekty továrny připojení, cílové objekty a dílčí kontexty.

Počáteční kontext se zobrazí v pohledu Navigator ve složce Spravované objekty produktu JMS . Všimněte si, že je-li zobrazen úplný obsah oboru názvů JNDI, v produktu MQ Explorer můžete upravovat pouze objekty IBM MQ classes for JMS , které jsou uloženy zde. Další informace naleznete v tématu [Přidání počátečního kontextu](#).

- Vytvořte a nakonfigurujte dílčí kontexty a spravované objekty JMS , které potřebujete.
Další informace naleznete v tématu [Vytvoření a konfigurace spravovaných objektů platformy JMS](#).
- Nakonfigurujte prostor IBM MQ.
Další informace naleznete v tématu [Konfigurace produktu IBM MQ pomocí produktu MQ Explorer](#) .

Související informace

[Úvod do produktu MQ Explorer](#)

[Vytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS](#)

Konfigurace objektů produktu JMS pomocí nástroje pro administraci

Pomocí nástroje pro administraci produktu IBM MQ JMS můžete definovat vlastnosti osmi typů objektů IBM MQ classes for JMS a uložit je do oboru názvů rozhraní JNDI. Aplikace pak mohou používat rozhraní JNDI k načtení těchto spravovaných objektů z oboru názvů.

Informace o této úloze

V následující tabulce jsou uvedeny osm typů spravovaných objektů, které lze vytvářet, konfigurovat a manipulovat s použitím příkazových slov. Sloupec Klíčové slovo zobrazuje řetězc, které můžete nahradit pro *TYPE* v příkazech zobrazených v [Tabulka 31](#) na stránce 486.

Tabulka 31. Typy objektů produktu JMS , které jsou zpracovány nástrojem pro administraci

Typ objektu	Klíčové slovo	Popis
MQConnectionFactory	CF	Implementace rozhraní IBM MQ rozhraní ConnectionFactory produktu JMS . Představuje objekt továrny pro vytvoření připojení v doménách typu point-to-point i publikování/odběr.
Továrna MQQueueConnection	QCF	Implementace produktu IBM MQ rozhraní továrny produktu JMS QueueConnection. To představuje objekt továrny pro vytvoření připojení v doméně dvoubodového spojení.
Továrna MQTopicConnection	TCF	Implementace produktu IBM MQ rozhraní továrny JMS TopicConnection. Tento objekt představuje objekt továrny pro vytváření připojení v doméně publikování/odběru.
MQQUEUE	Q	The IBM MQ implementation of the JMS Queue interface. Představuje místo určení pro zprávy v rámci domény typu point-to-point.
MQTopic	T	Implementace produktu IBM MQ rozhraní tématu produktu JMS . Představuje místo určení pro zprávy v doméně publikování/odběru.

Tabulka 31. Typy objektů produktu JMS , které jsou zpracovány nástrojem pro administraci (pokračování)

Typ objektu	Klíčové slovo	Popis
MQXAConnectionFactory “1” na stránce 487	XACF	Implementace rozhraní IBM MQ rozhraní JMS XAConnectionFactory . Představuje objekt továrny pro vytvoření připojení v doménách typu point-to-point i publikování/odběr a kde připojení používají verze XA pro třídy JMS .
Továrna MQXAQueueConnectionFactory “1” na stránce 487	XAQCF	Implementace produktu IBM MQ rozhraní továrny produktu JMS XAQueueConnection. Představuje objekt továrny pro vytvoření připojení v doméně dvoubodového spojení, které používají verze XA JMS tříd.
Továrna MQXATopicConnectionFactory “1” na stránce 487	XATCF	Implementace produktu IBM MQ rozhraní továrny produktu JMS XATopicConnection. Představuje objekt továrny pro vytváření připojení v doméně publikování/odběru, které používají verze XA pro JMS .

Poznámka:

1. Tyto třídy jsou k dispozici pro použití od dodavatelů aplikačních serverů. Je nepravděpodobné, že by byly pro programátory aplikací přímo užitečné.

Další informace o tom, jak nakonfigurovat tyto objekty, viz [“Konfigurace objektů produktu JMS” na stránce 494](#).

Typy vlastností a hodnoty, které je třeba použít k použití tohoto nástroje, jsou uvedeny v části [Vlastnosti objektů IBM MQ classes for JMS](#).

Tento nástroj můžete také použít k manipulaci s podkontexty oboru názvů adresáře v rámci rozhraní JNDI, jak je popsáno v tématu [“Konfigurace dílčích kontextů” na stránce 491](#).

Objekty spravované produktem JMS můžete také vytvářet a konfigurovat pomocí produktu MQ Explorer.

Související informace

[Vytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS](#)

[Použití JNDI k načtení spravovaných objektů v aplikaci JMS](#)

Konfigurace nástroje pro administraci produktu JMS

Nástroj pro administraci produktu IBM MQ JMS používá konfigurační soubor k nastavení hodnot určitých vlastností. K dispozici je ukázkový konfigurační soubor, který můžete upravit, aby vyhovoval vašemu systému.

Informace o této úloze

Konfigurační soubor je prostý textový soubor, který se skládá ze sady dvojic klíč-hodnota oddělených znakem rovnítko (=). Administrační nástroj nakonfigurujete nastavením hodnot pro tři vlastnosti definované v konfiguračním souboru. Následující příklad zobrazuje tyto tři vlastnosti:

```
#Set the service provider
INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
#Set the initial context
PROVIDER_URL=ldap://polaris/o=ibm_us,c=us
#Set the authentication type
SECURITY_AUTHENTICATION=none
```

(V tomto příkladu znak křížek (#) v prvním sloupci řádku označuje komentář, nebo řádek, který se nepoužívá.)

Ukázkový konfigurační soubor, který se používá jako výchozí konfigurační soubor, se dodává spolu s produktem IBM MQ. Ukázkový soubor se nazývá `JMSAdmin.config` nachází se v adresáři `<MQ_JAVA_INSTALL_PATH>/bin`. Buď můžete tento ukázkový soubor upravit, abyste definovali nastavení potřebná pro váš systém, nebo můžete vytvořit svůj vlastní konfigurační soubor.

Když spustíte nástroj pro administraci, můžete uvést konfigurační soubor, který chcete použít, pomocí parametru příkazového řádku `-cfg`, jak je popsáno v [“Spuštění nástroje pro administraci”](#) na stránce 489. Pokud při vyvolání nástroje nezadáte název konfiguračního souboru, nástroj se pokusí načíst výchozí konfigurační soubor (`JMSAdmin.config`). Prohledává tento soubor jako první v aktuálním adresáři a potom v adresáři `<MQ_JAVA_INSTALL_PATH>/bin`, kde `<MQ_JAVA_INSTALL_PATH>` je cesta k vaší instalaci produktu IBM MQ classes for JMS.


Názvy objektů produktu JMS, které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jedním z těchto konvencí je, že názvy objektu a kontextu musí obsahovat předponu, jako například `cn=` (obecný název) nebo `ou=` (organizační jednotka). Administrační nástroj zjednodušuje použití poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který dodáte. Pro protokol LDAP je to `cn=`. Je-li to nutné, můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru.

Poznámka: Možná budete muset nakonfigurovat server LDAP pro ukládání objektů Java. Další informace naleznete v dokumentaci k serveru LDAP.

Postup

1. Definujte poskytovatele služeb, kterého nástroj používá, konfigurací vlastnosti **INITIAL_CONTEXT_FACTORY**.

Podporované hodnoty této vlastnosti jsou následující:

- `com.sun.jndi.ldap.LdapCtxFactory` (pro LDAP)
- `com.sun.jndi.fscontext.RefFSContextFactory` (pro kontext systému souborů)
-  `com.ibm.jndi.LDAPCtxFactory` je podporováno pouze v systému z/OS a poskytuje přístup k serveru LDAP. Tato třída je však nekompatibilní s hodnotou `com.sun.jndi.ldap.LdapCtxFactory` v tom, že objekty vytvořené pomocí jednoho objektu `InitialContextFactory` nelze číst nebo upravovat pomocí druhého.

Administrační nástroj lze také použít k připojení k jiným kontextům rozhraní JNDI pomocí tří parametrů definovaných v konfiguračním souboru `JMSAdmin`. Chcete-li použít jinou továrnu `InitialContext`, postupujte takto:

- a) Nastavte vlastnost **INITIAL_CONTEXT_FACTORY** na požadovaný název třídy.
- b) Definujte chování továrny `InitialContextFactory` pomocí vlastností **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** a **NAME_READABILITY_MARKER**.

Nastavení pro tyto vlastnosti jsou popsány v komentářích ukázkového konfiguračního souboru.

Pokud použijete některou z podporovaných hodnot **INITIAL_CONTEXT_FACTORY**, není třeba definovat vlastnosti **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** a **NAME_READABILITY_MARKER**. Chcete-li však přepsat výchozí nastavení systému, můžete těmito vlastnostem dát hodnoty, chcete-li potlačit výchozí nastavení systému. Pokud jsou například vaše objekty uloženy v prostředí LDAP, můžete změnit výchozí předponu, kterou nástroj přidá k objektům a kontextovým názvům, nastavením vlastnosti **NAME_PREFIX** na požadovanou předponu.

Vynecháte-li jeden nebo více z těchto tří vlastností továrny `InitialContext`, nástroj pro administraci poskytne vhodné výchozí hodnoty založené na hodnotách ostatních vlastností.

2. Definujte adresu URL počátečního kontextu relace nakonfigurováním vlastnosti **PROVIDER_URL**.

Tato adresa URL je kořenem všech operací rozhraní JNDI, které nástroj provádí. Jsou podporovány dvě formy této vlastnosti:

- ldap://název_hostitele/kontextový_název
- file: [jednotka:] /název_cesty

Formát adresy URL protokolu LDAP se může lišit v závislosti na poskytovateli LDAP. Další informace naleznete v dokumentaci k protokolu LDAP.

3. Definujte, zda rozhraní JNDI předá pověření zabezpečení poskytovateli služeb nakonfigurováním vlastnosti **SECURITY_AUTHENTICATION**.

Tato vlastnost se používá pouze tehdy, je-li použit poskytovatel služby LDAP a může mít jednu ze tří hodnot:

Žádná (anonymní ověření)

Nastavíte-li tento parametr na hodnotu *none*, rozhraní JNDI nepředá žádné pověření zabezpečení poskytovateli služby a provede se *anonymní ověření*.

simple (jednoduché ověření)

Nastavíte-li tento parametr na hodnotu *simple*, budou pověření zabezpečení předávána prostřednictvím rozhraní JNDI základního poskytovatele služeb. Tato bezpečnostní pověření jsou ve formě rozlišovacího jména uživatele (DN uživatele) a hesla.

CRAM-MD5 (mechanismus ověření CRAM-MD5)

Nastavíte-li tento parametr na hodnotu *CRAM-MD5*, budou pověření zabezpečení předávána prostřednictvím rozhraní JNDI základního poskytovatele služeb. Tato bezpečnostní pověření jsou ve formě rozlišovacího jména uživatele (DN uživatele) a hesla.

Pokud nezádáte platnou hodnotu pro vlastnost **SECURITY_AUTHENTICATION**, výchozí hodnota vlastnosti je *none*.

Jsou-li požadována pověření zabezpečení, budete při inicializaci nástroje vyzváni k jejich zadání. Tomuto se lze vyhnout nastavením vlastností **PROVIDER_USERDN** a **PROVIDER_PASSWORD** v konfiguračním souboru `JMSAdmin`.

Poznámka: Pokud tyto vlastnosti nepoužijete, vypíše se na obrazovku text zadaný *včetně hesla*. To může mít dopad na zabezpečení.

Nástroj neprovádí žádné ověření; úloha ověření je delegována na server LDAP. Administrátor serveru LDAP musí nastavit a udržovat přístupová oprávnění k různým částem adresáře. Další informace naleznete v dokumentaci k protokolu LDAP. Pokud ověření selže, nástroj zobrazí odpovídající chybovou zprávu a ukončí se.

Podrobnější informace o zabezpečení a rozhraní JNDI najdete v dokumentaci na webových stránkách Oracle's Java ([Oracle Technology Network for Java Developers](http://www.oracle.com/technetwork/java/javadevelopers/)).

Spuštění nástroje pro administraci

Nástroj pro administraci má rozhraní příkazového řádku, které můžete použít buď interaktivně, nebo spustit dávkové zpracování.

Informace o této úloze

Interaktivní režim poskytuje příkazový řádek, kde můžete zadat příkazy administrace. V dávkovém režimu obsahuje příkaz ke spuštění nástroje název souboru, který obsahuje příkazový skript administrace.

Procedura

Interaktivní režim

- Chcete-li spustit nástroj v interaktivním režimu, zadejte tento příkaz:

```
JMSAdmin [-t] [-v] [-cfg config_filename]
```

kde:

-t

Povolí trasování (výchozí je trasování vypnuto).

Trasovací soubor je generován v produktu "%MQ_JAVA_DATA_PATH%\errors (Windows) nebo /var/mqm/trace (UNIX). Název trasovacího souboru je ve tvaru:

```
mjms_ PID.trc
```

kde *PID* je ID procesu prostředí JVM.

-v

Produkuje výstup s komentářem (výchozí hodnota je terse output)

-cfg název_konfiguračního_souboru

Název alternativního konfiguračního souboru. Je-li tento parametr vynechán, použije se výchozí konfigurační soubor `JMSAdmin.config`. Další informace o konfiguračním souboru viz téma [“Konfigurace nástroje pro administraci produktu JMS”](#) na stránce 487.

Zobrazí se příkazový řádek, který označuje, že je nástroj připraven přijímat příkazy administrace. Tato výzva se nejprve zobrazí jako:

```
InitCtx>
```

indikující, že aktuální kontext (tj. kontext JNDI, ke kterému se momentálně odkazují všechny operace pojmenovávání a adresářů), je počáteční kontext definovaný v konfiguračním parametru **PROVIDER_URL**. Další informace o tomto parametru naleznete v části [“Konfigurace nástroje pro administraci produktu JMS”](#) na stránce 487.

Při procházení oboru názvů adresáře se výzva k zobrazení této výzvy projeví, takže výzva k zadání vždy zobrazí aktuální kontext.

Dávkový režim

- Chcete-li spustit nástroj v dávkovém režimu, zadejte tento příkaz:

```
JMSAdmin <test.scf
```

kde `test.scf` je skriptový soubor, který obsahuje příkazy administrace. Další informace viz [“Použití příkazů administrace”](#) na stránce 490. Poslední příkaz v souboru musí být příkaz `END`.

Použití příkazů administrace

Nástroj pro správu přijímá příkazy skládající se z příkazového slova a jeho příslušných parametrů.

Informace o této úloze

Následující tabulka obsahuje seznam administrativních příkazových slov, které lze použít při zadávání příkazů s použitím administračního nástroje.

Sloveso	Krátký formát	Popis
ALTER	KLÁVES A ALT	Změnit alespoň jednu z vlastností spravovaného objektu
Definice	DEF	Vytvoření a uložení spravovaného objektu nebo vytvoření dílčího kontextu
DISPLAY	DIS	Zobrazit vlastnosti jednoho nebo více uložených spravovaných objektů nebo obsah aktuálního kontextu
ODSTRANIT	DEL	Odebrat jeden nebo více spravovaných objektů z oboru názvů nebo odebrat prázdný podkontext

Tabulka 32. Příkazová slova (pokračování)

Sloveso	Krátký formát	Popis
CHANGE	chg	Pozměnit aktuální kontext tak, aby uživatel mohl procházet obor názvů adresáře kdekoli pod počátečním kontextem (nevyřízená bezpečnostní prověrka)
COPY	CP	Vytvořit kopii uloženého spravovaného objektu a uložit jej pod alternativní název
MOVE	MV	Změnit název, pod kterým je spravovaný objekt uložen.
END		Zavřete nástroj pro administraci.

Procedura

- Není-li administrační nástroj již spuštěn, spusťte jej podle popisu v části [“Spuštění nástroje pro administraci”](#) na stránce 489.

Zobrazí se příkazový řádek, který označuje, že nástroj je připraven přijmout příkazy administrace. Tato výzva se nejprve zobrazí jako:

```
InitCtx>
```

Chcete-li změnit aktuální kontext, použijte příkaz CHANGE , jak je popsáno v tématu [“Konfigurace dílčích kontextů”](#) na stránce 491.

- Zadejte příkazy v následujícím tvaru:

```
verb [param]*
```

kde **verb** je jedním z administračních příkazových slov uvedených v Tabulka 32 na stránce 490. Všechny platné příkazy obsahují jedno příkazové slovo, které se objevuje na začátku příkazu buď ve standardním, nebo v krátkém tvaru. Názvy příkazů Verb nejsou citlivé na velikost písmen.

- Chcete-li ukončit příkaz, stiskněte klávesu Enter, pokud nechcete zadat několik příkazů najednou, v takovém případě zadejte znaménko plus (+) přímo před stisknutím klávesy Enter.

Chcete-li příkazy ukončit, stiskněte klávesu Enter. Tuto operaci však můžete potlačit zadáním znaku plus (+) před stisknutím klávesy Enter. To vám umožní zadat víceřádkové příkazy, jak je zobrazeno v následujícím příkladu:

```
DEFINE Q(BookingsInputQueue) +
QMGR(QM.POLARIS.TEST) +
QUEUE(BOOKINGS.INPUT.QUEUE) +
PORT(1415) +
CCSID(437)
```

- Chcete-li zavřít nástroj pro administraci, použijte příkazové slovo **END** . Toto slovo nemůže obsahovat žádné parametry.

Konfigurace dílčích kontextů

Chcete-li konfigurovat dílčí kontexty oboru názvů adresáře, můžete použít příkazy **CHANGE**, **DEFINE**, **DISPLAY** a **DELETE** .

Informace o této úloze

Použití těchto příkazových slov je popsáno v následující tabulce.

Tabulka 33. Syntaxe a popis příkazů používaných k manipulaci s podkontexty

Syntaxe příkazu	Popis
DEFINE CTX (ctxName)	Pokusí se o vytvoření podřízeného dílčího kontextu aktuálního kontextu s názvem ctxName. Pokud již existuje narušení zabezpečení, dojde k selhání zabezpečení, pokud již existuje, nebo není-li zadaný název platný.
ZOBRAZIT CTX	Zobrazí obsah aktuálního kontextu. Spravované objekty jsou anotovány pomocí a, dílčích kontextů s [D]. Zobrazí se také typ Java každého objektu.
ODSTRANIT CTX (ctxName)	Pokusy o odstranění podřízeného kontextu aktuálního kontextu s názvem ctxName. Pokud kontext nebyl nalezen, je neprázdný kontext nebo došlo k narušení zabezpečení.
CHANGE CTX (ctxName)	Pozměňuje aktuální kontext, takže se nyní odkazuje na podřízený kontext s názvem ctxName. Je možné zadat jednu ze dvou speciálních hodnot ctxName : = NAHORU přesunout na nadřízený prvek aktuálního kontextu = INICIALIZACE přesun přímo do počátečního kontextu Selhání, pokud určený kontext neexistuje, nebo pokud došlo k narušení zabezpečení.

Názvy objektů produktu JMS , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jedním z těchto konvencí je, že názvy objektu a kontextu musí obsahovat předponu, jako například cn= (obecný název) nebo ou= (organizační jednotka). Administrační nástroj zjednodušuje použití poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který dodáte. Pro protokol LDAP je to cn=. Je-li to nutné, můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru. Další informace viz [“Konfigurace nástroje pro administraci produktu JMS”](#) na stránce 487.

Poznámka: Možná budete muset nakonfigurovat server LDAP pro ukládání objektů Java . Další informace naleznete v dokumentaci k serveru LDAP.

Vytváření objektů JMS

Chcete-li vytvořit továrnu připojení JMS a cílové objekty a uložit je do oboru názvů JNDI, použijte příkazové slovo DEFINE . Chcete-li ukládat své objekty v prostředí LDAP, musíte jim dát názvy, které odpovídají určitým konvencím. Administrativní nástroj vám může pomoci dodržovat konvence pojmenování LDAP tím, že přidáte výchozí předponu k názvům objektů.

Informace o této úloze

Příkaz DEFINE vytváří administrovaný objekt s typem, názvem a vlastnostmi, které jste zadali. Nový objekt je uložen v aktuálním kontextu.

Názvy objektů produktu JMS , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jedním z těchto konvencí je, že názvy objektu a kontextu musí obsahovat předponu, jako například cn= (obecný název) nebo ou= (organizační jednotka). Administrační nástroj zjednodušuje použití poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který dodáte. Pro protokol LDAP je to cn=. Je-li to nutné, můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru. Další informace viz [“Konfigurace nástroje pro administraci produktu JMS”](#) na stránce 487.

Poznámka: Možná budete muset nakonfigurovat server LDAP pro ukládání objektů Java . Další informace naleznete v dokumentaci k serveru LDAP.

Postup

1. Není-li administrační nástroj již spuštěn, spusťte jej podle popisu v části [“Spuštění nástroje pro administraci”](#) na stránce 489.
Zobrazí se příkazový řádek, který označuje, že nástroj je připraven přijmout příkazy administrace.
2. Ujistěte se, že příkazový řádek zobrazuje kontext, ve kterém chcete vytvořit nový objekt.
Po spuštění nástroje pro administraci se na počátku zobrazí výzva k zadání jako:

```
InitCtx>
```

Chcete-li změnit aktuální kontext, použijte příkaz CHANGE , jak je popsáno v tématu [“Konfigurace dílčích kontextů”](#) na stránce 491.

3. Chcete-li vytvořit továrnu připojení, místo určení fronty nebo cíl tématu, použijte následující syntaxi příkazu:

```
DEFINE TYPE (name) [property]*
```

To znamená, že zadáte příkaz DEFINE a za ním následuje odkaz na spravovaný objekt TYPE (name) , následovaný nulou nebo více *vlastnostmi* (viz [Vlastnosti objektů IBM MQ classes for JMS](#)).

4. Chcete-li vytvořit továrnu připojení, místo určení fronty nebo cíl tématu, použijte následující syntaxi příkazu:

```
DEFINE TYPE (name) [property]*
```

5. Chcete-li zobrazit nově vytvořený objekt, použijte příkazové slovo DISPLAY s následující syntaxí příkazu:

```
DISPLAY TYPE (name)
```

Příklad

Následující příklad ukazuje frontu s názvem testQueue vytvořenou v počátečním kontextu pomocí příkazu DEFINE . Vzhledem k tomu, že tento objekt je ukládán v prostředí LDAP, ačkoli název objektu testQueue není zadán s předponou, nástroj automaticky přidá jeden k zajištění shody s konvencemi pojmenování LDAP. Zadání příkazu DISPLAY Q(testQueue) také způsobí, že se přidá tato předpona.

```
InitCtx> DEFINE Q(testQueue)
InitCtx> DISPLAY CTX
Contents of InitCtx
a cn=testQueue          com.ibm.mq.jms.MQQueue
1 Object(s)
0 Context(s)
1 Binding(s), 1 Administered
```

Ukázkové chybové stavy vytvářející objekt JMS

Při vytváření objektu může vzniknout řada běžných chybových stavů.

Níže jsou uvedeny příklady těchto chybových stavů:

CipherSpec mapována na CipherSuite

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SSLCIPHERSUITE(RC4_MD5_US)
WARNING: Converting CipherSpec RC4_MD5_US to
CipherSuite SSL_RSA_WITH_RC4_128_MD5
```

Neplatná vlastnost pro objekt

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PRIORITY(4)
Unable to create a valid object, please check the parameters supplied
Invalid property for a QCF: PRI
```

Neplatný typ hodnoty vlastnosti

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) CCSID(english)
Unable to create a valid object, please check the parameters supplied
Invalid value for CCS property: English
```

Konflikt vlastností-klient/bin.

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) HOSTNAME(polaris.hursley.ibm.com)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: Client-bindings attribute clash
```

Konflikt vlastností-inicializace uživatelské procedury

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SECEXITINIT(initStr)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: ExitInit string supplied
without Exit string
```

Hodnota vlastnosti mimo platný rozsah

```
InitCtx/cn=Trash> DEFINE Q(testQ) PRIORITY(12)
Unable to create a valid object, please check the parameters supplied
Invalid value for PRI property: 12
```

Neznámá vlastnost

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PIZZA(ham and mushroom)
Unable to create a valid object, please check the parameters supplied
Unknown property: PIZZA
```

Níže jsou uvedeny příklady chybových stavů, které se mohou vyskytnout na Windows při vyhledávání spravovaných objektů JNDI z aplikace JMS .

1. Pokud používáte poskytovatele JNDI WebSphere , com.ibm.websphere.naming.WsnInitialContextFactory, musíte použít dopředné lomítko (/) pro přístup ke spravovaným objektům definovaným v dílčích kontextech; například jms/MyQueueNázev. Použijete-li zpětné lomítko (\), dojde k výjimce InvalidName.
2. Používáte-li poskytovatele JNDI Oracle , com.sun.jndi.fscontext.RefFSContextFactory, musíte použít zpětné lomítko (\) pro přístup ke spravovaným objektům definovaným v dílčích kontextech; například ctx1\\fred. Použijete-li dopředné lomítko (/), dojde k NameNotFoundException .

Konfigurace objektů produktu JMS

Chcete-li manipulovat se spravovanými objekty v oboru názvů adresáře, můžete použít příkazy ALTER, DEFINE, DISPLAY, DELETE, COPY a MOVE .

Informace o této úloze

Tabulka 34 na stránce 495 shrnuje použití těchto příkazových slov. Nahrďte *TYPE* klíčovým slovem, které představuje požadovaný spravovaný objekt, jak je popsáno v [“Konfigurace objektů produktu JMS pomocí nástroje pro administraci”](#) na stránce 486.

Syntaxe příkazu	Popis
ALTER <i>TYPE</i> (název) [vlastnost] *	Pokusí se aktualizovat vlastnosti administrovaného objektu s dodanými objekty. Pokud došlo k narušení zabezpečení, selhání v případě, že uvedený objekt nebyl nalezen, nebo nejsou-li zadané nové vlastnosti platné.
DEFINE <i>TYP</i> (název) [vlastnost] *	Pokouší se vytvořit spravovaný objekt typu <i>TYPE</i> s dodanými vlastnostmi a uložit jej pod názvem name v aktuálním kontextu. Pokud je poskytnutý název neplatný nebo objekt s daným názvem existuje, nebo pokud zadané vlastnosti nejsou platné, došlo k selhání zabezpečení.
DISPLAY <i>TYP</i> (název)	Zobrazí vlastnosti spravovaného objektu typu <i>TYPE</i> s vazbou pod názvem name v aktuálním kontextu. Selhání, pokud objekt neexistuje, nebo pokud došlo k narušení zabezpečení.
DELETE <i>TYPE</i> (název)	Pokusí se odebrat administrovaný objekt typu <i>TYPE</i> , který má název name, z aktuálního kontextu. Selhání, pokud objekt neexistuje, nebo pokud došlo k narušení zabezpečení.
COPY <i>TYP</i> (nameA) <i>TYP</i> (nameB)	Vytvoří kopii spravovaného objektu typu <i>TYPE</i> s názvem nameA a pojmenovává se kopie nameB. Toto vše se vyskytuje v rozsahu aktuálního kontextu. Pokud objekt, který má být kopírován, neexistuje, existuje-li objekt s názvem nameB, nebo pokud dojde k narušení zabezpečení.
MOVE <i>TYPE</i> (nameA) <i>TYP</i> (nameB)	Přesouvá (přejmenovává) spravovaný objekt typu <i>TYPE</i> s názvem nameA na nameB. Toto vše se vyskytuje v rozsahu aktuálního kontextu. Pokud objekt, který má být přesunut, neexistuje, existuje-li objekt s názvem nameB, nebo pokud došlo k narušení zabezpečení.

Konfigurace prostředků produktu JMS v produktu WebSphere Application Server

Chcete-li konfigurovat prostředky produktu JMS v produktu WebSphere Application Server, můžete buď použít administrativní konzolu, nebo příkazy wsadmin.

Informace o této úloze

Aplikace produktu Java Message Service (JMS) obvykle závisí na externě nakonfigurovaných objektech, které popisují způsob, jakým se aplikace připojuje ke svému poskytovateli JMS a k místům určení, ke kterým přistupuje. Aplikace produktu JMS používají rozhraní Java Naming and Directory Interface (JNDI) pro přístup k následujícím typům objektů za běhu:

- Specifikace aktivace (používané aplikačními servery Java EE)
- Unifikované továrny připojení (s JMS 1.1, továrny na připojení nezávislé na doméně (unifikované) jsou preferovány pro továrny připojení fronty specifické pro doménu a továrny připojení témat)
- Továrny připojení tématu (používané aplikacemi produktu JMS 1.0)
- Továrny připojení fronty (používané aplikacemi produktu JMS 1.0)
- Fronty

- Témata

Through the IBM MQ messaging provider in WebSphere Application Server, Java Message Service (JMS) messaging applications can use your IBM MQ system as an external provider of JMS messaging resources. Chcete-li tento přístup povolit, nakonfigurujte poskytovatele systému zpráv produktu IBM MQ v produktu WebSphere Application Server za účelem definování prostředků produktu JMS pro připojení k libovolnému správci front v síti produktu IBM MQ .

Produkt WebSphere Application Server můžete použít ke konfiguraci prostředků produktu IBM MQ pro aplikace (například továrny připojení fronty) a ke správě zpráv a odběrů asociovaných s místy určení JMS . Zabezpečení budete spravovat prostřednictvím produktu IBM MQ .

Související informace pro produkt WebSphere Application Server verze 8.5.5

[Interoperace pomocí poskytovatele systému zpráv produktu IBM MQ](#)

[Správa systému zpráv s poskytovatelem systému zpráv produktu IBM MQ](#)

[Mapování názvů panelů administrativní konzoly na názvy příkazů a názvy IBM MQ](#)

Související informace pro WebSphere Application Server Verze 8.0

[Interoperace pomocí poskytovatele systému zpráv produktu IBM MQ](#)

[Správa systému zpráv s poskytovatelem systému zpráv produktu IBM MQ](#)

[Mapování názvů panelů administrativní konzoly na názvy příkazů a názvy IBM MQ](#)

Související informace pro WebSphere Application Server Verze 7.0

[Interoperace pomocí poskytovatele systému zpráv produktu IBM MQ](#)

[Správa systému zpráv s poskytovatelem systému zpráv produktu IBM MQ](#)

[Mapování názvů panelů administrativní konzoly na názvy příkazů a názvy IBM MQ](#)

Konfigurace prostředků produktu JMS pomocí administrativní konzoly

Administrativní konzolu produktu WebSphere Application Server můžete použít ke konfiguraci specifikací aktivity, továren připojení a cílů pro poskytovatele IBM MQ JMS .

Informace o této úloze

Administrativní konzolu produktu WebSphere Application Server můžete použít k vytvoření, zobrazení nebo úpravě libovolného z následujících prostředků:

- Specifikace aktivity
- Továrny na připojení nezávislé na doméně (JMS 1.1 nebo novější)
- Továrny připojení fronty
- Továrny připojení tématu
- Fronty
- Témata

Následující kroky poskytují přehled způsobů, jak pomocí administrativní konzoly konfigurovat prostředky produktu JMS pro použití s poskytovatelem systému zpráv produktu IBM MQ . Každý krok obsahuje název tématu v dokumentaci produktu WebSphere Application Server , na který se můžete podívat, abyste získali další informace. Odkazy na tato témata v dokumentaci produktu WebSphere Application Server 8.5.5, Verze 8.0 a Verze 7.0 najdete v tématu *Související odkazy* .

V buňce se smíšenými verzemi produktu WebSphere Application Server můžete spravovat prostředky produktu IBM MQ v uzlech všech verzí. Některé vlastnosti však nejsou k dispozici ve všech verzích. V této situaci jsou v administrativní konzole zobrazeny pouze vlastnosti daného uzlu.

Procedura

Chcete-li vytvořit nebo konfigurovat specifikaci aktivity pro použití s poskytovatelem systému zpráv produktu IBM MQ , postupujte takto:

- Chcete-li vytvořit specifikaci aktivace, použijte průvodce vytvořením prostředku produktu IBM MQ JMS .

Můžete buď použít průvodce k uvedení všech podrobností pro specifikaci aktivace, nebo můžete zvolit uvedení podrobností připojení pro IBM MQ pomocí tabulky CCDT (Client Channel Definition table). Když zadáte podrobnosti připojení pomocí průvodce, můžete zvolit buď zadání informací o hostiteli a portu samostatně, nebo, pokud používáte správce front s více instancemi, abyste mohli zadat informace o hostiteli a portu ve formě seznamu názvů připojení. Další informace naleznete v tématu *Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ*.

- Chcete-li zobrazit nebo změnit vlastnosti konfigurace specifikace aktivace, použijte panel nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ k administrativní konzole.

Tyto konfigurační vlastnosti řídí způsob vytváření připojení k přidruženým frontám a tématům. Další informace naleznete v tématu *Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li vytvořit nebo konfigurovat sjednocenou továrnu připojení, továrnu připojení fronty nebo továrnu připojení tématu pro použití s poskytovatelem systému zpráv produktu IBM MQ , postupujte takto:

- Chcete-li vytvořit továrnu na připojení, nejprve vyberte typ továrny připojení, který chcete vytvořit, a pak pomocí průvodce Vytvořit prostředek IBM MQ JMS určete podrobnosti.
 - Má-li aplikace JMS používat pouze dvoubodový systém zpráv, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv typu point-to-point, kterou lze použít pro vytváření připojení konkrétně pro systém zpráv typu point-to-point.
 - Je-li vaše aplikace produktu JMS určena pouze k použití systému zpráv publikování/odběru, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv publikování/odběru, kterou lze použít pro vytváření připojení speciálně pro systém zpráv publikování/odběru.
 - Pro produkt JMS 1.1 nebo novější vytvořte továrnu připojení nezávislou na doméně, kterou lze použít jak pro systém zpráv typu point-to-point, tak pro systém zpráv typu publikování/odběr, což umožňuje aplikaci provádět jak dvoubodové spojení, tak i publikování/odběr práce pod stejnou transakcí.

Můžete zvolit, zda se má průvodce použít k zadání všech podrobností pro továrnu připojení, nebo můžete určit podrobnosti o připojení pro produkt IBM MQ pomocí tabulky CCDT (Client Channel Definition table). Když zadáte podrobnosti připojení pomocí průvodce, můžete zvolit buď zadání informací o hostiteli a portu samostatně, nebo, pokud používáte správce front s více instancemi, abyste mohli zadat informace o hostiteli a portu ve formě seznamu názvů připojení. Další informace naleznete v tématu *Vytvoření továrny na připojení pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li zobrazit nebo změnit vlastnosti konfigurace faktorie připojení, postupujte takto:

- Pro typ továrny připojení, který chcete konfigurovat, použijte panel nastavení továrny připojení konzoly pro správu.

Konfigurační vlastnosti řídí způsob vytváření připojení k přidruženým frontám a tématům. Další informace naleznete v tématu *Konfigurace továrny na kolekce pro poskytovatele systému zpráv produktu IBM MQ* nebo *Konfigurace továrny kolekce fronty pro poskytovatele systému zpráv produktu IBM MQ* nebo *Konfigurace továrny kolekce témat pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li konfigurovat místo určení fronty JMS pro systém zpráv typu point-to-point s poskytovatelem systému zpráv produktu IBM MQ ,

- Panel nastavení fronty poskytovatele systému zpráv produktu IBM MQ administrativní konzoly slouží k definování následujících typů vlastností:
 - Obecné vlastnosti, včetně administračních a IBM MQ vlastností fronty.
 - Vlastnosti připojení, které určují způsob připojení ke správci front, který je hostitelem fronty.
 - Rozšířené vlastnosti, které řídí chování připojení k místům určení poskytovatele systému zpráv produktu IBM MQ .
 - Libovolné přizpůsobené vlastnosti pro místo určení fronty.

Další informace naleznete v tématu *Konfigurace fronty pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li vytvořit nebo nakonfigurovat místo určení tématu produktu JMS pro systém zpráv publikování/ odběru s poskytovatelem systému zpráv produktu IBM MQ , postupujte takto:

- Panel nastavení tématu poskytovatele systému zpráv produktu IBM MQ slouží k definování následujících typů vlastností:
 - Obecné vlastnosti, včetně administrace a vlastností témat IBM MQ .
 - Rozšířené vlastnosti, které řídí chování připojení k místům určení poskytovatele systému zpráv produktu IBM MQ .
 - Libovolné přizpůsobené vlastnosti pro místo určení fronty.

Další informace naleznete v tématu *Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ*.

Související pojmy

[“Tabulka definic kanálů klienta” na stránce 37](#)

Tabulka definic kanálů klienta (CCDT) určuje definice kanálu a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformách jiných než z/OS je tabulka CCDT vytvořena automaticky. Poté jej musíte zpřístupnit klientské aplikaci.

[“Správci front s více instancemi” na stránce 401](#)

Správci front s více instancemi jsou instance stejného správce front konfigurovaného na různých serverech. Jedna instance správce front je definována jako aktivní instance a jiná instance je definována jako instance v pohotovostním režimu. Dojde-li k selhání aktivní instance, správce front s více instancemi se automaticky restartuje na záložním serveru.

[“Konfigurace publikování/odběru zpráv” na stránce 329](#)

Můžete spustit, zastavit a zobrazit stav publikování/odběru ve frontě. Můžete také přidávat a odebírat proudy a přidávat a odstraňovat správce front z hierarchie zprostředkovatele.

Související informace pro produkt WebSphere Application Server verze 8.5.5

[Specifikace aktivace poskytovatele systému zpráv produktu IBM MQ](#)

[Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ](#)

[Vytvoření továrny na připojení pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace sjednocené továrny připojení pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace továrny připojení fronty pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace továrny připojení tématu pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace fronty pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ](#)

Související informace pro WebSphere Application Server Verze 8.0

[Specifikace aktivace poskytovatele systému zpráv produktu IBM MQ](#)

[Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ](#)

[Vytvoření továrny na připojení pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace sjednocené továrny připojení pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace továrny připojení fronty pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace továrny připojení tématu pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace fronty pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ](#)

Související informace pro WebSphere Application Server Verze 7.0

[Specifikace aktivace poskytovatele systému zpráv produktu IBM MQ](#)

[Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ](#)

[Vytvoření továrny na připojení pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace sjednocené továrny připojení pro poskytovatele systému zpráv produktu IBM MQ](#)

[Konfigurace továrny připojení fronty pro poskytovatele systému zpráv produktu IBM MQ](#)
[Konfigurace továrny připojení tématu pro poskytovatele systému zpráv produktu IBM MQ](#)
[Konfigurace fronty pro poskytovatele systému zpráv produktu IBM MQ](#)
[Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ](#)

Konfigurace prostředků produktu JMS pomocí skriptovacích příkazů nástroje wsadmin

You can use WebSphere Application Server wsadmin scripting commands to create, modify, delete or show information about JMS activation specifications, connection factories, queues and topics. Můžete také zobrazit a spravovat nastavení pro adaptér prostředků produktu IBM MQ .

Informace o této úloze

Následující kroky poskytují přehled způsobů, jak pomocí příkazů wsadmin wsadmin WebSphere Application Server konfigurovat prostředky produktu JMS pro použití s poskytovatelem systému zpráv produktu IBM MQ . Další informace o použití těchto příkazů naleznete v tématu *Související odkazy* , kde najdete odkazy na dokumentaci produktu WebSphere Application Server verze 8.5.5, Verze 8.0 a Verze 7.0 .

Chcete-li spustit příkaz, použijte objekt AdminTask skriptovacího klienta wsadmin.

Po použití příkazu k vytvoření nového objektu nebo k provedení změn uložte provedené změny do hlavní konfigurace. Použijte například následující příkaz:

```
AdminConfig.save()
```

Chcete-li zobrazit seznam dostupných administrativních příkazů poskytovatele systému zpráv produktu IBM MQ a stručný popis jednotlivých příkazů, zadejte na příkazový řádek nástroje wsadmin následující příkaz:

```
print AdminTask.help('WMQAdminCommands')
```

Chcete-li zobrazit přehlednou nápovědu k danému příkazu, zadejte na příkazový řádek nástroje wsadmin následující příkaz:

```
print AdminTask.help('command_name')
```

Procedura

Chcete-li vypsat všechny prostředky poskytovatele systému zpráv produktu IBM MQ definované v oboru, ve kterém je příkaz zadán, použijte následující příkazy.

- Chcete-li vypsat specifikace aktivace, použijte příkaz **listWMQActivationSpecs** .
- Chcete-li vypsat seznam továren připojení, použijte příkaz **listWMQConnectionFactory** .
- Chcete-li vypsat cíle typu fronty, použijte příkaz **listWMQQueues** .
- Chcete-li zobrazit seznam míst určení typu tématu, použijte příkaz **listWMQTopics** .

Chcete-li vytvořit prostředek produktu JMS pro poskytovatele systému zpráv produktu IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li vytvořit specifikaci aktivace, použijte příkaz **createWMQActivationSpec** .
Můžete buď vytvořit specifikaci aktivace zadáním všech parametrů, které mají být použity pro vytvoření připojení, nebo můžete vytvořit specifikaci aktivace tak, aby používala tabulku definic kanálů klienta (CCDT) k vyhledání správce front, k němuž se má připojit.
- Chcete-li vytvořit továrnu připojení, použijte příkaz **createWMQConnectionFactory** s použitím parametru **-type** k určení typu továrny připojení, kterou chcete vytvořit:

- Má-li aplikace JMS používat pouze dvoubodový systém zpráv, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv typu point-to-point, kterou lze použít pro vytváření připojení konkrétně pro systém zpráv typu point-to-point.
- Je-li vaše aplikace produktu JMS určena pouze k použití systému zpráv publikování/odběru, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv publikování/odběru, kterou lze použít pro vytváření připojení speciálně pro systém zpráv publikování/odběru.
- Pro produkt JMS 1.1 nebo novější vytvořte továrnu připojení nezávislou na doméně, kterou lze použít jak pro systém zpráv typu point-to-point, tak pro systém zpráv typu publikování/odběr, což umožňuje aplikaci provádět jak dvoubodové spojení, tak i publikování/odběr práce pod stejnou transakcí.

Výchozí typ je továrna připojení nezávislá na doméně.

- Chcete-li vytvořit místo určení typu fronty, použijte příkaz **createWMQQueue** .
- Chcete-li vytvořit místo určení typu tématu, použijte příkaz **createWMQTopic** .

Chcete-li upravit prostředek produktu JMS pro poskytovatele systému zpráv produktu IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li upravit specifikaci aktivace, použijte příkaz **modifyWMQActivationSpec** .
Typ specifikace aktivace nelze změnit. Například, nemůžete vytvořit specifikaci aktivace, do které zadáte všechny informace o konfiguraci ručně, a pak ji upravit tak, aby používala tabulku CCDT.
- Chcete-li upravit továrnu připojení, použijte příkaz **modifyWMQConnectionFactory** .
- Chcete-li upravit místo určení typu fronty, použijte příkaz **modifyWMQQueue** .
- Chcete-li upravit místo určení typu tématu, použijte příkaz **modifyWMQTopic** .

Chcete-li odstranit prostředek produktu JMS pro poskytovatele systému zpráv produktu IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li odstranit specifikaci aktivace, použijte příkaz **deleteWMQActivationSpec** .
- Chcete-li odstranit továrnu připojení, použijte příkaz **deleteWMQConnectionFactory** .
- Chcete-li odstranit cíl typu fronty, použijte příkaz **deleteWMQQueue** .
- Chcete-li odstranit místo určení typu tématu, použijte příkaz **deleteWMQTopic** .

Chcete-li zobrazit informace o specifickém prostředku poskytovatele systému zpráv produktu IBM MQ , použijte následující příkazy.

- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k určité specifikaci aktivace, použijte příkaz **showWMQActivationSpec** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k určité faktorii připojení, použijte příkaz **showWMQConnectionFactory** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k určitému místu určení typu fronty, použijte příkaz **showWMQQueue** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k místu určení typu tématu, použijte příkaz **showWMQTopic** .

Chcete-li spravovat nastavení pro adaptér prostředků produktu IBM MQ nebo pro poskytovatele systému zpráv produktu IBM MQ , použijte následující příkazy.

- Chcete-li spravovat nastavení adaptéru prostředků produktu IBM MQ , který je instalován v určitém oboru, použijte příkaz **manageWMQ** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty, které lze nastavit pomocí příkazu **manageWMQ** , použijte příkaz **showWMQ** . Tato nastavení se vztahují buď k adaptéru prostředků produktu IBM MQ , nebo k poskytovateli systému zpráv produktu IBM MQ . Příkaz **showWMQ** také zobrazuje všechny přízpusobené vlastnosti, které jsou nastaveny na adaptéru prostředků IBM MQ .

Související pojmy

[“Tabulka definic kanálů klienta” na stránce 37](#)

Tabulka definic kanálů klienta (CCDT) určuje definice kanálu a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformách jiných než z/OS je tabulka CCDT vytvořena automaticky. Poté jej musíte zpřístupnit klientské aplikaci.

“Správci front s více instancemi” na stránce 401

Správci front s více instancemi jsou instance stejného správce front konfigurovaného na různých serverech. Jedna instance správce front je definována jako aktivní instance a jiná instance je definována jako instance v pohotovostním režimu. Dojde-li k selhání aktivní instance, správce front s více instancemi se automaticky restartuje na záložním serveru.

“Konfigurace publikování/odběru zpráv” na stránce 329

Můžete spustit, zastavit a zobrazit stav publikování/odběru ve frontě. Můžete také přidávat a odebírat proudy a přidávat a odstraňovat správce front z hierarchie zprostředkovatele.

Související informace pro produkt WebSphere Application Server verze 8.5.5

[createWMQActivationSpec](#) příkaz

[createWMQConnectionFactory](#) příkaz

[createWMQQueue](#) příkaz

[createWMQTopic](#) příkaz

[deleteWMQActivationSpec](#) příkaz

[deleteWMQConnectionFactory](#) příkaz

[deleteWMQQueue](#) příkaz

[deleteWMQTopic](#) příkaz

[listWMQActivationSpecs](#) příkaz

[listWMQConnectionFactories](#) příkaz

[listWMQQueues](#) příkaz

[listWMQTopics](#) příkaz

[modifyWMQActivationSpec](#) příkaz

[modifyWMQConnectionFactory](#) příkaz

[modifyWMQQueue](#) příkaz

[modifyWMQTopic](#) příkaz

[showWMQActivationSpec](#) příkaz

[showWMQConnectionFactory](#) příkaz

[showWMQQueue](#) příkaz

[showWMQTopic](#) příkaz

[showWMQ](#) příkaz

[manageWMQ](#) příkaz

Související informace pro WebSphere Application Server Verze 8.0

[createWMQActivationSpec](#) příkaz

[createWMQConnectionFactory](#) příkaz

[createWMQQueue](#) příkaz

[createWMQTopic](#) příkaz

[deleteWMQActivationSpec](#) příkaz

[deleteWMQConnectionFactory](#) příkaz

[deleteWMQQueue](#) příkaz

[deleteWMQTopic](#) příkaz

[listWMQActivationSpecs](#) příkaz

[listWMQConnectionFactories](#) příkaz

[listWMQQueues](#) příkaz

[listWMQTopics](#) příkaz

[modifyWMQActivationSpec](#) příkaz

[modifyWMQConnectionFactory](#) příkaz

[modifyWMQQueue](#) příkaz

[modifyWMQTopic](#) příkaz
[showWMQActivationSpec](#) příkaz
[showWMQConnectionFactory](#) příkaz
[showWMQQueue](#) příkaz
[showWMQTopic](#) příkaz
[showWMQ](#) příkaz
[manageWMQ](#) příkaz
Související informace pro WebSphere Application Server Verze 7.0
[createWMQActivationSpec](#) příkaz
[createWMQConnectionFactory](#) příkaz
[createWMQQueue](#) příkaz
[createWMQTopic](#) příkaz
[deleteWMQActivationSpec](#) příkaz
[deleteWMQConnectionFactory](#) příkaz
[deleteWMQQueue](#) příkaz
[deleteWMQTopic](#) příkaz
[listWMQActivationSpecs](#) příkaz
[listWMQConnectionFactories](#) příkaz
[listWMQQueues](#) příkaz
[listWMQTopics](#) příkaz
[modifyWMQActivationSpec](#) příkaz
[modifyWMQConnectionFactory](#) příkaz
[modifyWMQQueue](#) příkaz
[modifyWMQTopic](#) příkaz
[showWMQActivationSpec](#) příkaz
[showWMQConnectionFactory](#) příkaz
[showWMQQueue](#) příkaz
[showWMQTopic](#) příkaz
[showWMQ](#) příkaz
[manageWMQ](#) příkaz

Konfigurace aplikačního serveru pro použití nejnovější úrovně údržby adaptéru prostředků

Chcete-li zajistit automatickou aktualizaci adaptéru prostředků produktu IBM MQ na nejnovější dostupnou úroveň údržby při použití opravných sad produktu WebSphere Application Server , můžete nakonfigurovat všechny servery ve svém prostředí tak, aby používaly nejnovější verzi adaptéru prostředků obsaženou v sadě oprav produktu WebSphere Application Server , kterou jste použili při instalaci jednotlivých uzlů.

Než začnete

Důležité: Používáte-li produkt WebSphere Application Server Verze 7.0 verze 8 nebo verze 8.5 na libovolné platformě, neinstalujte adaptér prostředků produktu IBM MQ 8.0 na aplikační server. Adaptér prostředků produktu IBM MQ 8.0 lze implementovat pouze na aplikační server, který podporuje produkt JMS 2.0. Produkt WebSphere Application Server verze 7.0, verze 8 a verze 8.5 však podporuje pouze JMS 1.1. Tyto verze produktu WebSphere Application Server jsou dodávány s adaptérem prostředků produktu IBM WebSphere MQ 7.0 , který lze použít k připojení ke správci front produktu IBM MQ 8.0 pomocí přenosu BINDINGS nebo CLIENT.

Informace o této úloze

Tuto úlohu použijte, pokud se na vaši konfiguraci vztahuje kterákoliv z následujících okolností a vy chcete nakonfigurovat všechny servery ve vašem prostředí pro použití nejnovější verze adaptéru prostředků IBM MQ :

- Protokoly prostředí JVM libovolného aplikačního serveru ve vašem prostředí zobrazí po použití produktu WebSphere Application Server Verze 7.0 s opravou FixPack 1 nebo novější následující informace o verzi adaptéru prostředků produktu IBM MQ :

```
Implementace WMSG1703I:RAR Verze 7.0.0.0-k700-L080820
```

- Protokoly JVM všech aplikačních serverů ve vašem prostředí obsahují následující položku:

```
WMSG1625E: Nebylo možné zjistit  
Kód poskytovatele systému zpráv produktu IBM MQ na zadané cestě < null>
```

- Jeden nebo více uzlů bylo dříve ručně aktualizováno tak, aby používalo specifickou úroveň údržby adaptéru prostředků produktu IBM MQ , který je nyní nahrazený nejnovější verzí adaptéru prostředků obsaženého v aktuální úrovni údržby produktu WebSphere Application Server .

Adresář *profile_root* , na který se příklady odkazují, je domovským adresářem profilu produktu WebSphere Application Server , například C:\Program Files\IBM\WebSphere\AppServer1.

Po provedení následujících kroků pro všechny buňky a instalace jediného serveru ve vašem prostředí budou servery při použití nové opravné sady produktu WebSphere Application Server automaticky přijímat údržbu adaptéru prostředků produktu IBM MQ .

Postup

1. Spustíte aplikační server. Je-li profil součástí konfigurace síťové implementace, spustíte správce implementace a všechny agenty uzlů. Pokud profil obsahuje administrativního agenta, spustíte administrativního agenta.
2. Zkontrolujte úroveň údržby adaptéru prostředků produktu IBM MQ .
 - a) Otevřete okno příkazového řádku a přejděte do adresáře *profile_root*\bin .
Zadejte například `cd C:\Program Files\IBM\WebSphere\AppServer1\bin`.
 - b) Spustíte nástroj wsadmin tak, že zadáte příkaz `wsadmin.bat -lang jython`, a pak, pokud jste k tomu vyzváni, zadejte své jméno uživatele a heslo.
 - c) Napište následující příkaz a pak dvakrát klávesu Return:

```
wmqInfoMBeansUnsplit = AdminControl.queryNames("WebSphere:type=WmqInfo,*")  
wmqInfoMBeansSplit = AdminUtilities.convertToList(wmqInfoMBeansUnsplit)  
for wmqInfoMBean in wmqInfoMBeansSplit: print wmqInfoMBean; print AdminControl.invoke(wmqInfoMBean,  
'getInfo', '')
```

Tento příkaz můžete také spustit v jazyce Jacl. Další informace o tom, jak to provést, najdete v tématu *Zajištění toho, aby servery používaly nejnovější dostupnou úroveň údržby adaptéru prostředků produktu IBM MQ* v dokumentaci produktu WebSphere Application Server .

- d) Najděte zprávu WMSG1703I ve zobrazeném výstupu z příkazu a zkontrolujte úroveň adaptéru prostředků.

Například pro produkt WebSphere Application Server Verze 7.0 Fixpack 15 by měla být zpráva:

```
WMSG1703I: Implementace RAR Verze 7.0.1.3-k701-103-100812
```

Tato zpráva zobrazuje, že verze je 7.0.1.3-k701-103-100812, což je správná úroveň adaptéru prostředků pro tuto opravnou sadu. Pokud se však místo toho zobrazí následující zpráva, znamená to, že je třeba upravit adaptér prostředků na správnou úroveň údržby pro opravnou sadu 15.

```
WMSG1703I: Implementace RAR Verze 7.0.0.0-k700-L080820
```

3. Zkopírujte následující skript Jython do souboru s názvem `convertWMQRA.py` poté jej uložte do kořenového adresáře profilu, například C:\Program Files\IBM\WebSphere\AppServer1\bin.

```
ras = AdminUtilities.convertToList(AdminConfig.list('J2CResourceAdapter'))  
for ra in ras :
```

```

desc = AdminConfig.showAttribute(ra, "description")
if (desc == "WAS 7.0 Built In IBM MQ Resource Adapter") or (desc == "WAS 7.0.0.1 Built In IBM MQ
Resource Adapter"):
    print "Updating archivePath and classpath of " + ra
    AdminConfig.modify(ra, [['archivePath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar]])
    AdminConfig.unsetAttributes(ra, ['classpath'])
    AdminConfig.modify(ra, [['classpath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar]])
    AdminConfig.save()
#end if
#end for

```

Tip: Při ukládání souboru se ujistěte, že je soubor uložen jako soubor python, nikoli jako textový soubor.

4. Use the WebSphere Application Server wsadmin tool to run the Jython script that you have just created.

Otevřete příkazový řádek a přejděte do adresáře `\bin` v domovském adresáři pro WebSphere Application Server, například adresář `C:\Program Files\IBM\WebSphere\AppServer1\bin`, poté zadejte následující příkaz a stiskněte klávesu Return:

```
wsadmin -lang jython -f convertWMQRA.py
```

Pokud k tomu budete vyzváni, zadejte své jméno uživatele a heslo.

Poznámka: Spustíte-li skript pro profil, který je součástí konfigurace síťové implementace, skript aktualizuje všechny profily, které v této konfiguraci potřebují aktualizaci. Úplná resynchronizace může být nutná, pokud již existují nekonzistence konfiguračního souboru.

5. Pracujete-li v konfiguraci síťové implementace, ujistěte se, že jsou agenti uzlů plně resynchronizováni. Další informace naleznete v tématu Synchronizace uzlů pomocí skriptovacího nástroje wsadmin nebo Přidání, správa a odebrání uzlů.
6. Zastavte všechny servery v profilu. Je-li profil součástí konfigurace síťové implementace, zastavte také všechny členy klastru v konfiguraci, zastavte všechny agenty uzlu v konfiguraci a zastavte správce implementace. Pokud profil obsahuje administrativního agenta, zastavte administrativního agenta.
7. Spusťte příkaz **osgiCfgInit** z adresáře `profile_root/bin`.
Příkaz `osgiCfgInit` resetuje mezipaměť třídy používanou běhovým prostředím OSGi. Je-li profil součástí konfigurace síťové implementace, spusťte příkaz **osgiCfgInit** z adresáře `profile_root/bin` každého profilu, který je součástí konfigurace.
8. Restartujte všechny servery v profilu. Je-li profil součástí konfigurace síťové implementace, můžete také restartovat všechny členy klastru v konfiguraci, restartovat všechny agenty uzlů v konfiguraci a restartovat správce implementace. Pokud profil obsahuje administrativního agenta, restartujte administrativního agenta.
9. Zopakujte krok 2 a zkontrolujte, zda je adaptér prostředků nyní na správné úrovni.

Jak pokračovat dále

Budete-li po provedení kroků popsaných v tomto tématu i nadále docházet k problémům a dříve jste použili tlačítko **Aktualizovat adaptér prostředků** na panelu Nastavení poskytovatele serveru JMS v administrativní konzole serveru WebSphere Application Server, abyste aktualizovali adaptér prostředků produktu IBM MQ na všech uzlech ve vašem prostředí, je možné, že se vyskytl problém popsaný v tématu APAR PM10308.

Související informace

[Použití adaptéru prostředků produktu IBM MQ](#)

Související informace pro produkt WebSphere Application Server verze 8.5.5

[Zajištění toho, aby servery používaly nejnovější dostupnou úroveň údržby adaptéru prostředků produktu IBM MQ](#)

[Synchronizace uzlů pomocí skriptovacího nástroje wsadmin](#)

[Přidání, správa a odebírání uzlů](#)

[Nastavení poskytovatele služeb JMS](#)

Související informace pro WebSphere Application Server Verze 8.0

[Zajištění toho, aby servery používaly nejnovější dostupnou úroveň údržby adaptéru prostředků produktu IBM MQ](#)

[Synchronizace uzlů pomocí skriptovacího nástroje wsadmin](#)

[Přidání, správa a odebírání uzlů](#)

[Nastavení poskytovatele služeb JMS](#)

Související informace pro WebSphere Application Server Verze 7.0

[Zajištění toho, aby servery používaly nejnovější dostupnou úroveň údržby adaptéru prostředků produktu IBM MQ](#)

[Synchronizace uzlů pomocí skriptovacího nástroje wsadmin](#)

[Přidání, správa a odebírání uzlů](#)

[Nastavení poskytovatele služeb JMS](#)

Konfigurace vlastnosti produktu JMS PROVIDERVERSION

Poskytovatel systému zpráv produktu IBM MQ má tři režimy provozu: normální režim, normální režim s omezeními a režim migrace. Můžete nastavit vlastnost JMS **PROVIDERVERSION**, abyste vybrali, který z těchto režimů používá aplikace JMS k publikování a odběru.

Informace o této úloze

Výběr způsobu operace poskytovatele systému zpráv produktu IBM MQ lze primárně řídit nastavením vlastnosti továrny připojení PROVIDERVERSION. Režim operace může být také vybrán automaticky, pokud režim nebyl zadán.

Vlastnost **PROVIDERVERSION** rozlišuje mezi třemi režimy poskytovatele systému zpráv produktu IBM MQ :

Normální režim poskytovatele systému zpráv produktu IBM MQ

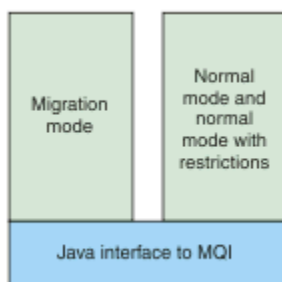
Normální režim používá všechny funkce správce front IBM MQ k implementaci služby JMS. Tento režim je optimalizovaný pro použití rozhraní API a funkčnosti produktu JMS 2.0 .

IBM MQ s omezeními

Normální režim s omezeními používá rozhraní API produktu JMS 2.0 , ale ne nové funkce, tj. sdílené odběry, odložené doručení a asynchronní odeslání.

Režim migrace poskytovatele systému zpráv produktu IBM MQ

Pomocí režimu migrace se můžete připojit ke správci front produktu IBM MQ 8.0 , ale nejsou použity žádné funkce správce front produktu IBM WebSphere MQ 7.0 nebo novější, jako je například dopředné čtení a kontinuální načítání.



Obrázek 84. Režimy poskytovatele systému zpráv

Procedura

Chcete-li konfigurovat vlastnost **PROVIDERVERSION** pro specifickou továrnu připojení, postupujte takto:

- Chcete-li nakonfigurovat vlastnost produktu **PROVIDERVERSION** pomocí produktu MQ Explorer, viz téma [Konfigurace správců front a objektů](#).

- Chcete-li nakonfigurovat vlastnost **PROVIDERVERSION** pomocí administračního nástroje produktu JMS , přečtěte si téma [Konfigurace správců front a objektů](#).
- Chcete-li nakonfigurovat vlastnost **PROVIDERVERSION** v aplikaci JMS pomocí rozšíření produktu IBM JMS nebo rozšíření IBM MQ JMS , prostudujte si téma [Vytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS](#).

Chcete-li potlačit nastavení režimu poskytovatele továrny připojení pro všechny továrny připojení v prostředí JVM, postupujte takto:

- Chcete-li potlačit nastavení režimu poskytovatele továrny připojení, použijte vlastnost `com.ibm.msg.client.wmq.overrideProviderVersion`.
Pokud nemůžete změnit vámi používanou továrnu připojení, můžete pomocí vlastnosti `com.ibm.msg.client.wmq.overrideProviderVersion` přepsat libovolné nastavení v továrně připojení. Tento přepis platí pro všechny továrny připojení v prostředí JVM, ale skutečné objekty továrny připojení se nezmění.

Související informace

[PROVIDERVERSION](#)

[Odstraňování problémů s verzí poskytovatele JMS](#)

[Vlastnosti továrny připojení](#)

[Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS](#)

Režimy poskytovatele systému zpráv produktu IBM MQ

Můžete si vybrat, který z těchto režimů operace použije aplikace JMS k publikování a odběru nastavením vlastnosti **PROVIDERVERSION** pro továrnu připojení na příslušnou hodnotu. V některých případech je vlastnost **PROVIDERVERSION** nastavena jako nespecifikovaná, v takovém případě klient JMS používá algoritmus k určení, jaký režim operace použít.

PROVIDERVERSION Hodnoty vlastností

Vlastnost továrny připojení **PROVIDERVERSION** můžete nastavit na některou z následujících hodnot:

8 - Normální režim

Aplikace JMS používá normální režim. Tento režim používá všechny funkce správce front produktu IBM MQ k implementaci produktu JMS.

7 - Normální režim s omezeními

Aplikace JMS používá normální režim s omezeními. Tento režim používá rozhraní JMS 2.0 API, ale ne nové funkce, jako sdílení odběrů, odložené doručení nebo asynchronní odeslání.

6-režim migrace

Aplikace JMS používá režim migrace. V režimu migrace používá produkt IBM MQ classes for JMS funkce a algoritmy podobné těm, které jsou dodávány s produktem IBM WebSphere MQ 6.0.

neurčeno (výchozí hodnota)

Klient JMS používá algoritmus k určení, který režim operace se používá.

Vámi zadaná hodnota ve vlastnosti **PROVIDERVERSION** musí být řetězec. Pokud zadáte volbu 8, 7 nebo 6, můžete to provést v některém z následujících formátů:

- V.R.M.F
- V.R.M
- V.R
- V

kde V, R, M a F jsou celá čísla větší nebo rovná nule. Hodnoty R, M a F jsou nepovinné a můžete je použít k upřesnění v případě potřeby řízení s vysokou úrovní granularity. Chcete-li například použít úroveň **PROVIDERVERSION** z 7, můžete nastavit **PROVIDERVERSION** = 7, 7.0, 7.0.0 nebo 7.0.0.0.

Typy objektů továrny připojení

Vlastnost **PROVIDERVERSION** lze nastavit pro následující typy objektů továrny připojení:

- MQConnectionFactory
- Továrna MQQueueConnection
- Továrna MQTopicConnection
- MQXAConnectionFactory
- Továrna MQXAQueueConnection
- Továrna MQXAQueueConnection
- Továrna MQXAQueueConnection
- Továrna MQXATopicConnection

Další informace o těchto různých typech továrny připojení najdete v tématu [“Konfigurace objektů produktu JMS pomocí nástroje pro administraci”](#) na stránce 486.

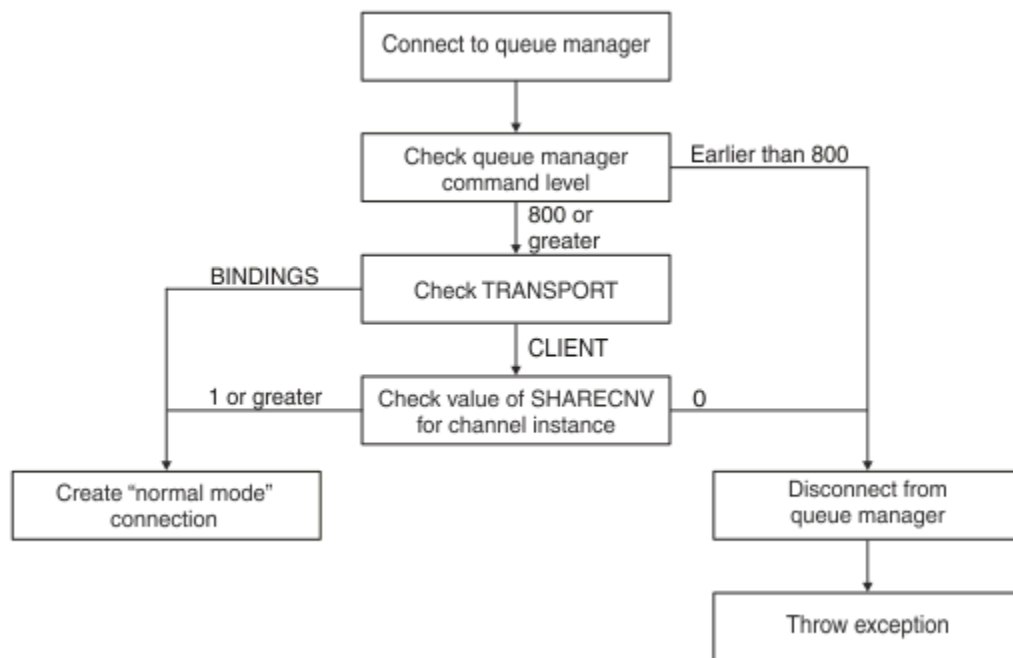
Související informace

[Architektura produktu IBM MQ pro architekturu JMS](#)

PROVIDERVERSION Normální režim

Normální režim používá všechny funkce správce front IBM MQ k implementaci služby JMS. Tento režim je optimalizovaný pro použití rozhraní API a funkčnosti produktu JMS 2.0 .

Následující graf toku zobrazuje kontroly, které klient JMS provádí k určení, zda lze vytvořit normální připojení režimu.



Obrázek 85. Normální režim PROVIDERVERSION

Je-li správce front určený v nastavení továrny připojení nastaven na úroveň 800 nebo vyšší a vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS, bude vytvořeno normální připojení režimu bez kontroly dalších vlastností.

Pokud má správce front uvedený v nastavení továrny připojení úroveň příkazů 800 nebo vyšší a vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, bude zkontrolována také vlastnost **SHARECNV** na kanálu připojení serveru. Tato kontrola je nutná, protože poskytovatel systému zpráv produktu IBM MQ v normálním režimu používá funkci sdílení konverzací. Proto je pro pokus o připojení normálního režimu

úspěšný pokus o vlastnost **SHARECNV** , která určuje počet konverzací, které lze sdílet, musí mít hodnotu 1 nebo vyšší.

Pokud jsou všechny kontroly zobrazené ve vývojovém diagramu úspěšné, lze použít normální připojení režimu ke správci front a všechny funkce rozhraní API a funkce produktu JMS 2.0 , tj. asynchronní odeslání, zpožděné doručení a sdílené odběry, lze poté použít.

Pokus o vytvoření připojení v normálním režimu selhává z následujících příčin:

- Správce front uvedený v nastavení továrny připojení má úroveň příkazů, která je starší než 800. V tomto případě metoda `createConnection` selže s výjimkou `JMSFMQ0003`.
- Vlastnost **SHARECNV** na kanálu připojení serveru je nastavena na hodnotu 0. Pokud tato vlastnost nemá hodnotu 1 nebo vyšší, metoda `createConnection` selže s výjimkou `JMSCC5007`.

Související informace

Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

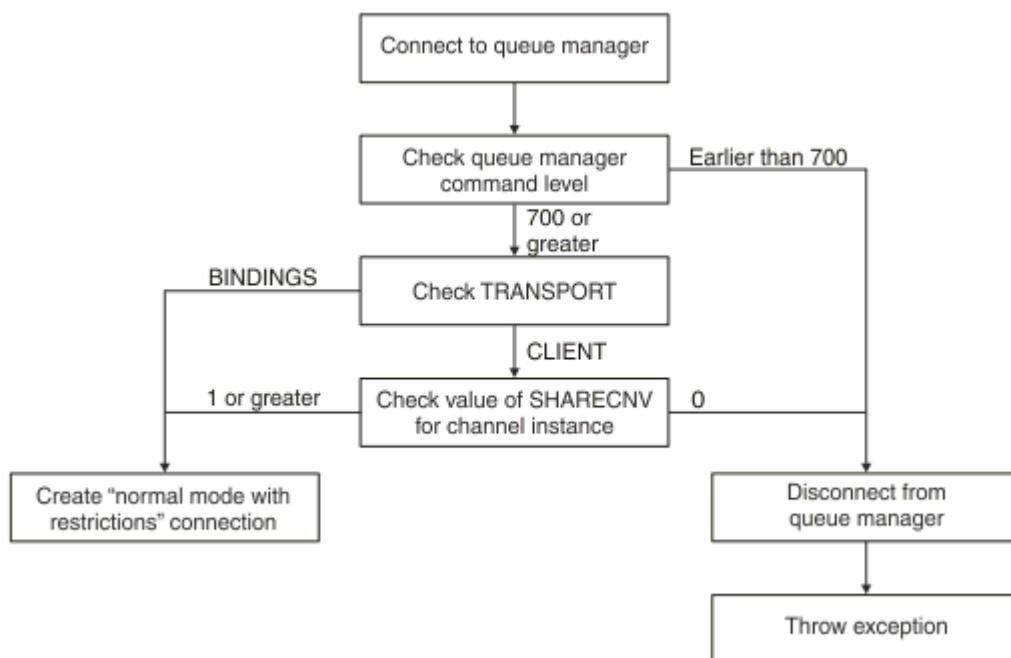
DEFINE CHANNEL (vlastnost SHARECNV)

TRANSPORT

Normální režim PROVIDERVERSION s omezeními

Normální režim s omezeními používá rozhraní API JMS 2.0 , ale ne nové funkce produktu IBM MQ 8.0 , jako jsou sdílené odběry, odložené doručení nebo asynchronní odeslání.

Následující graf toku zobrazuje kontroly, které klient JMS provádí k určení, zda lze vytvořit normální režim s omezením připojení.



Obrázek 86. Normální režim PROVIDERVERSION s omezeními

Je-li správce front zadaný v nastavení továrny připojení nastaven na hodnotu 700 nebo vyšší a vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu `BINDINGS`, bude vytvořeno připojení v normálním režimu bez kontroly dalších vlastností.

Má-li správce front zadaný v nastavení továrny připojení úroveň příkazu 700 nebo vyšší a vlastnost **TRANSPORT** je nastavena na hodnotu `CLIENT`, bude zkontrolována také vlastnost **SHARECNV** na kanálu připojení serveru. Tato kontrola je nutná, protože poskytovatel systému zpráv produktu IBM MQ v normálním režimu s omezeními používá funkci sdílení konverzací. Proto musí mít vlastnost **SHARECNV** , která řídí počet konverzací, které lze sdílet, hodnotu 1 nebo větší, pro normální režim s pokusem o omezení připojení.

Pokud jsou všechny kontroly zobrazené ve vývojovém diagramu úspěšné, vytvoří se normální režim s omezením připojení ke správci front a vy pak můžete použít rozhraní API JMS 2.0 , ale ne asynchronní odeslání, odložené doručení nebo sdílené funkce odběru.

Pokus o vytvoření normálního režimu s omezováním připojení selhává z následujících důvodů:

- Správce front uvedený v nastavení továrny připojení má úroveň příkazů, která je starší než 700. V tomto případě se metoda `createConnection` nezdaří s výjimkou `JMSFCC5008`.
- Vlastnost **SHARECNV** na kanálu připojení serveru je nastavena na hodnotu 0. Pokud tato vlastnost nemá hodnotu 1 nebo vyšší, metoda `createConnection` selže s výjimkou `JMSCC5007`.

Související informace

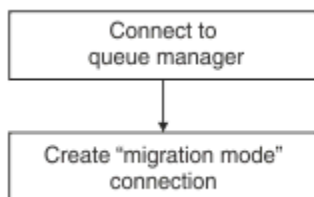
Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

DEFINE CHANNEL (vlastnost SHARECNV)

TRANSPORT

Režim migrace produktu PROVIDERVERSION

Pro režim migrace používá produkt IBM MQ classes for JMS funkce a algoritmy podobné těm, které jsou dodávány s produktem IBM WebSphere MQ 6.0, jako je publikování/odběr ve frontě, výběr implementovaný na straně klienta, nemultiplexové kanály a systém výzev používaný k implementaci listenerů.



Obrázek 87. Migrační režim PROVIDERVERSION

Chcete-li se připojit k produktu WebSphere Message Broker Verze 6.0 nebo 6.1 pomocí produktu IBM MQ Enterprise Transport Verze 6.0, musíte použít režim migrace.

Pomocí režimu migrace se můžete připojit ke správci front produktu IBM MQ 8.0 , ale žádná z nových funkcí správce front produktu IBM MQ classes for JMS se nepoužívá, například dopředné čtení nebo kontinuální načítání. Pokud máte klienta IBM MQ 8.0 připojícího se ke správci front produktu IBM MQ 8.0 na distribuované platformě nebo správci front IBM MQ 8.0 v systému z/OS, pak je výběr zpráv proveden spíše správcem front, než v systému klienta.

Je-li zadán režim migrace poskytovatele systému zpráv produktu IBM MQ a IBM MQ classes for JMS se pokusí použít některý z rozhraní API produktu JMS 2.0 , volání metody rozhraní API se nezdaří s výjimkou `JMSCC5007`.

Související informace

Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

TRANSPORT

PROVIDERVERSION nspecifikováno

Není-li vlastnost **PROVIDERVERSION** továrny připojení určena, klient JMS používá algoritmus k určení, který režim operace se používá pro připojení ke správci front. Továrna připojení, která byla vytvořena v oboru názvů JNDI s předchozí verzí produktu IBM MQ classes for JMS , vezme neurčenou hodnotu, je-li továrna připojení použita s novou verzí produktu IBM MQ classes for JMS.

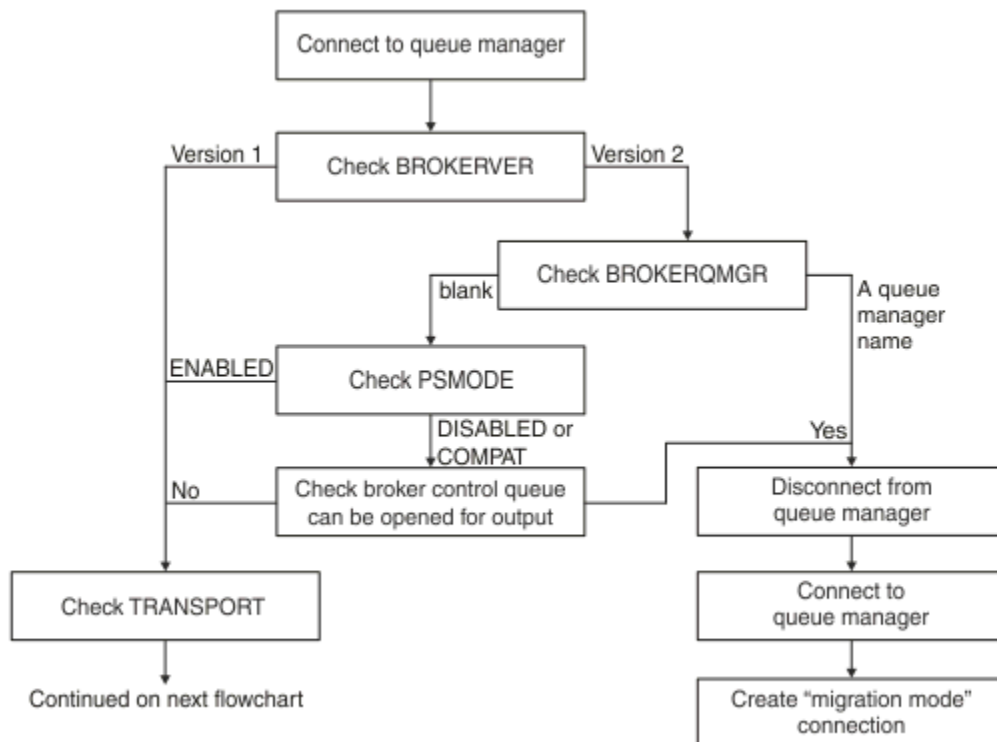
Není-li vlastnost **PROVIDERVERSION** určena, je algoritmus použit při volání metody `createConnection` . Algoritmus kontroluje určitý počet vlastností továrny připojení a určuje, zda je vyžadován normální režim poskytovatele systému zpráv produktu IBM MQ , normální režim s omezeními nebo režim migrace poskytovatele systému zpráv produktu IBM MQ . Normální režim se vždy nejprve pokusí o první režim a pak normální režim s omezeními. Pokud nelze vytvořit ani jeden z těchto typů

připojení, odpojí se klient JMS od správce front a potom se znovu připojí ke správci front, aby se pokusil o připojení v režimu migrace.

Kontrola vlastností produktů BROKERVER, BROKERQMGR, PSMODE a BROKERCONQ

Kontrola hodnot vlastností začíná vlastností **BROKERVER**, jak ukazuje Obrázek 1.

Je-li vlastnost **BROKERVER** nastavena na hodnotu V1, bude vlastnost **TRANSPORT** se zaškrtnutá jako další, jak ukazuje Obrázek 2. Je-li však vlastnost **BROKERVER** nastavena na hodnotu V2, další kontrola zobrazená na Obrázku 1 se provádí před kontrolou vlastnosti **TRANSPORT**.



Obrázek 88. PROVIDERVERZE není

Je-li vlastnost **BROKERVER** nastavena na hodnotu V2, musí být vlastnost **BROKERQMGR** pro normální připojení režimu prázdná. Kromě toho musí být atribut **PSMODE** ve správci front nastaven na hodnotu **ENABLED** nebo nesmí být otevřena řídicí fronta zprostředkovatele určená vlastností **BROKERCONQ** pro výstup.

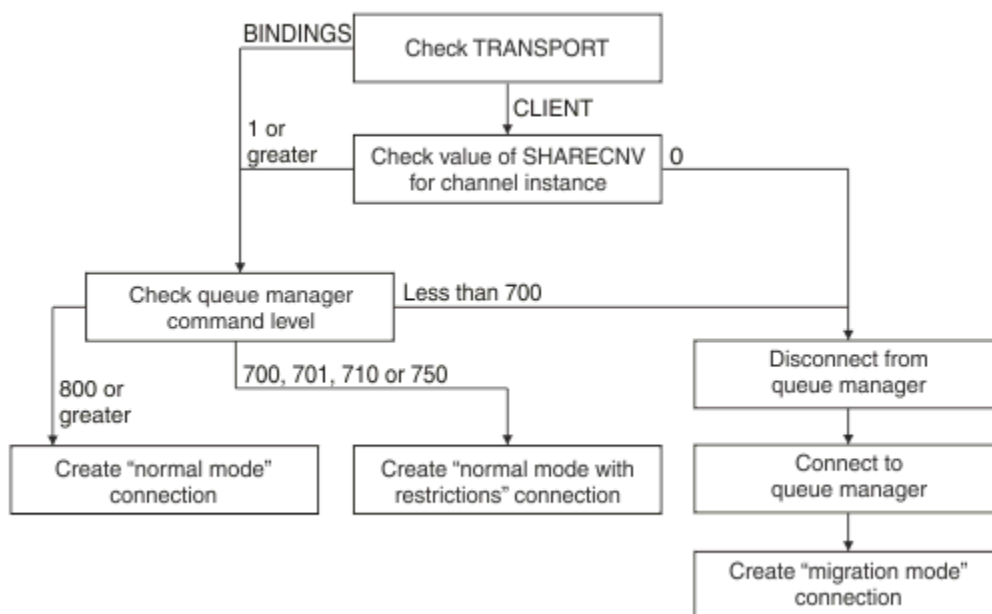
Jsou-li hodnoty vlastností nastaveny jako vyžadované pro normální připojení režimu, kontrola dalšího se přesune na vlastnost **TRANSPORT**, jak ukazuje Obrázek 2.

Nejsou-li hodnoty vlastností nastaveny jako vyžadované pro normální připojení režimu, klient JMS se odpojí od správce front a poté se znovu připojí a vytvoří připojení režimu migrace. K tomu dojde v následujících případech:

- Pokud je vlastnost **BROKERQMGR** blank a atribut **PSMODE** na správci front je nastaven na hodnotu **COMPAT** nebo **DISABLED** a fronta řízení zprostředkovatele zadaná vlastností **BROKERCONQ** může být otevřena pro výstup (to znamená, že výstup **MQOPEN** je úspěšný).
- Pokud vlastnost **BROKERQMGR** uvádí název fronty.

Kontrola vlastnosti TRANSPORT a úrovně příkazu

Obrázek 2 zobrazuje kontroly provedené pro vlastnost **TRANSPORT** a úroveň příkazů správce front.



Obrázek 89. PROVIDERVERSION nespecifikováno (pokračování)

Připojení normální režim je vytvořeno v jednom z následujících případů:

- Vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS a správce front má úroveň příkazů 800 nebo vyšší.
- Vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, vlastnost **SHARECNV** kanálu připojení k serveru má hodnotu 1 nebo vyšší a správce front má úroveň příkazů 800 nebo vyšší.

Má-li správce front úroveň příkazů 700, 701, 710 nebo 750, vytvoří se normální režim s omezením připojení ke správci front.

Má-li správce front nižší úroveň příkazů než 700, odpojí se klient JMS od správce front a potom se znovu připojí ke správci front, aby vytvořil připojení režimu migrace.

Připojení v režimu migrace se také vytvoří, pokud je vlastnost **TRANSPORT** nastavena na hodnotu CLIENT a vlastnost **SHARECNV** kanálu připojení serveru má hodnotu 0.

Související informace

Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

[ALTER QMGR \(atribut PSMODE\)](#)

[BROKERCONQ](#)

[BROKERQMGR](#)

[BROKERVER](#)

[DEFINE CHANNEL \(vlastnost SHARECNV\)](#)

[TRANSPORT](#)

Kdy přepsat výchozí nastavení PROVIDERVERSION

Je-li továrna připojení vytvořená v oboru názvů JNDI s předchozí verzí produktu IBM MQ classes for JMS použita s novou verzí produktu IBM MQ classes for JMS, vlastnost **PROVIDERVERSION** pro továrnu připojení je nastavena na výchozí hodnotu `unspecified` a používá se k určení, který režim poskytovatele systému zpráv produktu IBM MQ se používá. Avšak existují dva případy, kdy musíte přepsat výchozí výběr pro vlastnost **PROVIDERVERSION**, aby mohl produkt IBM MQ classes for JMS pracovat správně.

Poznámka: Režim migrace, který je popsán v tomto tématu, je pro migraci z produktu IBM WebSphere MQ 6.0 do produktu IBM WebSphere MQ 7.0. Nevztahuje se na migraci z novějších vydání.

IBM WebSphere MQ 6.0, WebSphere Application Server Verze 6.0.x a WebSphere Message Broker Verze 6 jsou mimo podporu, a proto je toto téma zahrnuto pouze pro referenční účely.

Je-li vlastnost **PROVIDERVERSION** nastavena na výchozí hodnotu `unspecified`, algoritmus se používá k určení, jaký režim operace použít, jak je popsáno v [“PROVIDERVERSION nespecifikováno”](#) na stránce 509. Tento algoritmus však nelze použít v následujících dvou scénářích.

1. Pokud jsou WebSphere Message Broker a WebSphere Event Broker v režimu kompatibility, musíte zadat hodnotu pro vlastnost **PROVIDERVERSION**, aby WebSphere Message Broker a WebSphere Event Broker fungovaly správně.
2. Pokud používáte WebSphere Application Server Verze 6.00,1, WebSphere Application Server Verze 6.0.2 nebo WebSphere Application Server Verze 6.1, továrny připojení jsou definovány pomocí administrativní konzoly serveru WebSphere Application Server.

V produktu WebSphere Application Server je výchozí hodnota vlastnosti **BROKERVER** v továrně připojení V2. Výchozí hodnota vlastnosti **BROKERVER** pro továrny připojení, které jsou vytvořeny pomocí nástroje pro administraci produktu JMS **JMSAdmin** nebo MQ Explorer je V1. Tato vlastnost je nyní nespecifikovaná v produktu IBM MQ.

Pokud je vlastnost **BROKERVER** nastavena na hodnotu V2, protože byla vytvořena produktem WebSphere Application Server nebo byla použita továrna připojení pro publikování/odběr před a má existujícího správce front, který má definovanou vlastnost produktu **BROKERCONQ** (protože byla použita pro systém zpráv publikování/odběru), je použit režim migrace poskytovatele systému zpráv produktu IBM MQ.

Pokud však chcete, aby aplikace používala komunikaci typu P2P a aplikace používá existujícího správce front, který byl někdy použit pro publikování/odběr, a má továrnu připojení s hodnotou **BROKERVER** nastavenou na hodnotu 2, což je výchozí nastavení, pokud byla továrna připojení vytvořena v produktu WebSphere Application Server, bude použit režim migrace poskytovatele systému zpráv produktu IBM MQ. Použití režimu migrace poskytovatele systému zpráv produktu IBM MQ v tomto případě není nutné; místo toho použijte normální režim poskytovatele systému zpráv produktu IBM MQ. K práci můžete použít jednu z následujících metod:

- Nastavte **BROKERVER** na 1 nebo nespecifikované. Volba, kterou zvolíte, závisí na aplikaci.
- Nastavte **PROVIDERVERSION** na 8, nebo 7, což jsou přizpůsobené vlastnosti v produktu WebSphere Application Server Verze 6.1.

Případně můžete použít vlastnost konfigurace klienta nebo upravit připojení správce front tak, aby nepoužíval sadu vlastností **BROKERCONQ**, nebo tuto frontu nepoužívat.

Konfigurace informací o verzi poskytovatele v produktu WebSphere Application Server

Chcete-li konfigurovat informace o verzi poskytovatele v produktu WebSphere Application Server, můžete buď použít administrativní konzolu, nebo příkazy `wsadmin`.

Postup

Chcete-li konfigurovat informace o verzi poskytovatele pro továrnu připojení nebo objekt specifikace aktivace produktu IBM MQ v produktu WebSphere Application Server, viz *Související informace*, kde najdete odkazy na další informace v dokumentaci produktu WebSphere Application Server.

Související informace pro produkt WebSphere Application Server verze 8.5.5

[Nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ](#)

`createWMQConnectionFactory` příkaz

[Nastavení specifikace aktivace poskytovatele systému zpráv produktu IBM MQ](#)

`createWMQActivationSpec` příkaz

Související informace pro WebSphere Application Server Verze 8.0.0

[Nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ](#)

`createWMQConnectionFactory` příkaz

[Nastavení specifikace aktivace produktu IBM MQ](#)

createWMQActivationSpec příkaz

Související informace pro WebSphere Application Server Verze 7.0.0

Nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ

createWMQConnectionFactory příkaz

Nastavení specifikace aktivace produktu IBM MQ

createWMQActivationSpec příkaz

Odebrání trvalých odběrů produktu WebSphere Application Server verze 7 a verze 8

Při použití poskytovatele systému zpráv produktu WebSphere MQ s produktem WebSphere Application Server verze 7 a verze 8 nejsou odebrány trvalé odběry vytvořené aplikacemi objektů typu message-driven bean, které jsou svázány se specifikacemi aktivace. Trvalé odběry lze odebrat buď pomocí programu Průzkumník produktu MQ, nebo pomocí obslužného programu příkazového řádku WebSphere MQ.

Informace o této úloze

Aplikace typu message-driven bean spuštěné v produktu WebSphere Application Server verze 7 a verze 8, které používají produkt Normální režim poskytovatele systému zpráv produktu WebSphere MQ k připojení k produktu WebSphere MQ a k odběru trvalého odběru, lze konfigurovat tak, aby používaly buď porty modulu listener, nebo specifikace aktivace.

Je-li aplikace objektu typu message-driven bean svázána s portem modulu listener, poskytovatel systému zpráv WebSphere MQ při prvním spuštění aplikace vytvoří trvalý odběr pro aplikaci. Trvalý odběr bude odebrán při odinstalaci aplikace objektu bean řízeného zprávami z aplikačního serveru a po restartu aplikačního serveru.

Aplikace typu message-driven bean, které jsou svázány se specifikací aktivace, fungují mírně odlišným způsobem. Trvalý odběr je vytvořen pro aplikaci při prvním spuštění aplikace. Trvalý odběr však nebude odebrán při odinstalaci aplikace a restartování aplikačního serveru.

To může vést k řadě trvalých odběrů, které zůstanou na serveru WebSphere MQ Publish/Subscribe pro aplikaci, které již nejsou instalovány v systému WebSphere Application Server. Tyto odběry jsou známy jako "osiřelé odběry" a mohou vést k problémům ve správci front, je-li stroj publikování/odběru spuštěn.

Je-li zpráva publikována v tématu, stroj publikování/odběru produktu WebSphere MQ vytvoří kopii této zprávy pro každý trvalý odběr registrovaný v daném tématu a vloží jej do interní fronty. Aplikace, které používají tento trvalý odběr, budou poté vyzvednou a spotřebovávají zprávu z této interní fronty.

Pokud aplikace typu message-driven bean, která používala tento trvalý odběr, již není nainstalována, budou nadále prováděny kopie publikovaných zpráv pro danou aplikaci. Tyto zprávy však nebudou nikdy zpracovány, což znamená, že ve vnitřní frontě může být velký počet zpráv, které nebudou nikdy odebrány.

Než začnete

Odběry, které jsou registrovány s produktem WebSphere MQ Publish/Subscribe Engine, budou mít k sobě přidružené názvy odběru.

Durable subscriptions created by the WebSphere Application Server WebSphere MQ messaging provider for message-driven beans that are bound to activation specifications will have a Subscription Name in the following format:

```
JMS:<queue manager name>:<client identifier>:<subscription name>
```

Kde:

<název správce front>

Jedná se o název správce front produktu WebSphere MQ, na kterém je spuštěn stroj publikování/odběru.

<identifikátor klienta>

Jedná se o hodnotu vlastnosti ID klienta ve specifikaci aktivace, na kterou je objekt typu message-driven bean svázán.

<název odběru>

Jedná se o hodnotu názvu odběru vlastnosti specifikace aktivace pro specifikaci aktivace, kterou byla konfigurována aplikace objektu typu message driven bean pro použití.

Předpokládejme například, že máme specifikaci aktivace, která byla nastavena pro připojení ke správci front testQM. Specifikace má nastaveny následující vlastnosti:

- ID klienta = testClientID
- Název odběru = durableSubscription1

Je-li objekt typu message-driven bean, který trvá na trvalém odběru, svázán s touto specifikací aktivace, vytvoří se odběr na serveru WebSphere MQ publish/subscribe u správce front testQM, který má následující název odběru:

- JMS:testQM:testClientID:durableSubscription1

Odběry, které byly registrovány s produktem WebSphere MQ publish/subscribe Engine pro daného správce front, lze zobrazit jedním z následujících dvou způsobů:

- První možností je použití Průzkumníka produktu MQ. Pokud byl program Průzkumník produktu MQ připojen ke správci front používanému k publikování/odběru, lze zobrazit seznam odběratelů, kteří jsou aktuálně registrováni u publikování/odběru stroje publikování, klepnutím na položku IBM WebSphere MQ -><queue manager name>-> Subscriptions v navigačním podokně.
- Druhým způsobem, jak zobrazit odběry registrované pomocí stroje publikování/odběru, je použití příkaz runmqsc příkazového řádku produktu WebSphere MQ a spustit příkaz **display sub**. Chcete-li tak učinit, vyvolejte příkazový řádek, přejděte do adresáře <WebSphere MQ> \bin a zadejte následující příkaz ke spuštění příkazu runmqsc:

– runmqsc <queue manager name>

Po spuštění obslužného programu runmqsc zadejte následující příkaz k vypsání všech trvalých odběrů, které jsou aktuálně registrovány v rámci stroje publikování/odběru spuštěných ve správci front, ke kterému došlo k připojení příkazu runmqsc:

– display sub(*) durable

Chcete-li zkontrolovat, zda jsou trvalé odběry registrované s generátory publikování/odběru stále aktivní:

1. Generujte seznam trvalých odběrů, které byly registrovány s použitím stroje publikování/odběru.
2. Pro každý trvalý odběr:

- Podívejte se na název odběru pro trvalého odběratele a poznamenejte si hodnotu < identifikátor klienta > a < název odběru >.
- Podívejte se na systémy aplikačního serveru WebSphere Application Server, které se připojují k tomuto stroji publikování/odběru. Zjistěte, zda existují nějaké definované specifikace aktivace, které mají vlastnost ID klienta, která odpovídá hodnotě < identifikátor klienta > a vlastnosti názvu odběru, která odpovídá < název odběru >.
- Pokud nejsou nalezeny žádné specifikace aktivace s vlastnostmi ID klienta a názvu odběru, které odpovídají polím < client identifier > a < subscription name > v názvu odběru WebSphere MQ, neexistují žádné specifikace aktivace s použitím tohoto trvalého odběru. Trvalý odběr lze odstranit.
- Je-li definována specifikace aktivace, která odpovídá názvu trvalého odběru, bude provedena konečná kontrola, kterou je třeba provést, je-li k dispozici aplikace typu message-driven bean používající tuto specifikaci aktivace. Postupujte takto:
 - Poznamenejte si název rozhraní JNDI pro specifikaci aktivace, která odebrala trvalý odběr, v němž se aktuálně hledáte.
 - Vyved'te podokno Konfigurace v administrativní konzole WebSphere pro každou aplikaci typu message-driven bean, která byla nainstalována.

- V podokně Konfigurace klepněte na odkaz na vazby modulu listener objektu typu message driven bean.
- Zobrazí se tabulka s informacemi o aplikaci objektu typu message driven bean. Je-li ve sloupci Vazby vybrán přepínač specifikace aktivace a v poli Název rozhraní JNDI cílového prostředku je uveden název rozhraní JNDI pro specifikaci aktivace, která odebrala trvalý odběr, je odběr nadále používán a nelze jej odstranit.
- Pokud nelze nalézt žádné aplikace typu message-driven bean, které používají specifikaci aktivace, lze trvalý odběr odstranit.

Postup

Jakmile je identifikován "osiřelý" trvalý odběr, lze jej odstranit buď pomocí Průzkumníka MQ , nebo pomocí obslužného programu příkazového řádku WebSphere MQ **runmqsc**.

Chcete-li odstranit "osiřelý" trvalý odběr pomocí Průzkumníka MQ , postupujte takto:

1. Zvýraznit položku pro odběr
2. Klepněte pravým tlačítkem myši na položku a vyberte volbu **Odstranit ...** z nabídky. Zobrazí se okno s potvrzením.
3. Zkontrolujte správnost názvu odběru zobrazeného v okně s potvrzením a klepněte na tlačítko **Ano**.

Průzkumník produktu MQ nyní odstraní odběr z stroje publikování/odběru a vyčistí všechny vnitřní prostředky, které jsou k němu přidruženy (jako jsou nezpracované zprávy publikované pro téma, na kterém byl registrován trvalý odběr).

To delete an "orphaned" durable subscription using the WebSphere MQ command line utility **runmqsc**, the command **delete sub** must be run:

1. Otevřít relaci příkazového řádku
2. Přejděte do adresáře <WebSphere MQ> \bin
3. Zadejte následující příkaz ke spuštění produktu **runmqsc**:

```
runmqsc <queue manager name>
```

4. Po spuštění obslužného programu **runmqsc** zadejte:

```
delete sub(<Subscription name>)
```

kde <Název odběru> je název odběru trvalého odběru, který má podobu:

- JMS:<queue manager name>:<client identifier>:<subscription name>

Konfigurace produktu HP Integrity NonStop Server

Tyto informace vám pomohou při konfiguraci klienta IBM MQ HP Integrity NonStop Server pro instalaci produktu HP Integrity NonStop Server .

Podrobnosti o konfiguraci klienta pomocí konfiguračního souboru viz [“Konfigurace klienta pomocí konfiguračního souboru”](#) na stránce 47.

Podrobnosti o konfiguraci klienta pomocí proměnných prostředí naleznete v tématu [“Použití proměnných prostředí IBM MQ”](#) na stránce 71.

Pokud provádíte klienta produktu IBM MQ HP Integrity NonStop Server pro operace produktu HP Integrity NonStop Server pod TMF/Gateway, prohlédněte si podtémata pro informace o tom, jak nakonfigurovat TMF/Gateway. Zahrnutý je přehled procesu brány, konfigurace brány pro spuštění pod cestou Pathway a konfigurace inicializačního souboru klienta pro povolení klienta IBM MQ HP Integrity NonStop Server pro produkt HP Integrity NonStop Server pro přístup k bráně TMF Gateway.

Tato sekce obsahuje také klienta IBM MQ HP Integrity NonStop Server pro HP Integrity NonStop Server specifické informace o udělování oprávnění k kanálům.

Přehled procesu brány

Produkt HP NonStop Transaction Management Facility (TMF) poskytuje služby, které umožňují procesu brány zaregistrovat se jako správce prostředků. Proces IBM WebSphere MQ for HP Integrity NonStop Server poskytovaný TMF/Gateway běží pod cestou Pathway.

Produkt IBM WebSphere MQ for HP Integrity NonStop Server registruje jeden proces brány pro každého správce front, který je koordinován TMF, proto musíte nakonfigurovat samostatný TMF/Gateway pro každého správce front, který se bude účastnit koordinovaných jednotek práce TMF. Tato registrace je tak, že každý správce front je nezávislý správce prostředků, a pro administrativní účely registrace každého správce front jednou s produktem HP NonStop TMF výsledků v snadno srozumitelném mapování.

V případě více instalací produktu IBM WebSphere MQ for HP Integrity NonStop Server musíte navrhnout jeden proces brány z jedné z těchto instalací pro každého správce front, který bude koordinován TMF.

Rozhraní procesu brány podporuje všechny klienty stejné nebo starší verze.

Další informace o administraci procesu brány naleznete v tématu [Administrace produktu HP Integrity NonStop Server](#).

Konfigurace brány pro spuštění pod cestou Pathway

TMF/Gateway je rozhraní mezi rozhraním HP NonStop Transaction Management Facility (TMF) a IBM MQ, které umožňuje TMF být koordinátorem transakcí pro transakce IBM MQ.

Produkt IBM MQ poskytuje TMF/Gateway konvertuje transakce z koordinace TMF do koordinace transakcí architektury eXtended Architecture (XA) pro komunikaci se vzdáleným správcem front.

Musíte mít jednoho TMF/Gateway pro správce front, který vyžaduje koordinaci, a je vyžadována konfigurace klienta, aby se klient mohl připojit ke správné bráně.

TMF/Gateway může použít všechny mechanismy dostupné klientovi ke komunikaci se správcem front. Nakonfigurujte TMF/Gateway způsobem, který chcete použít pro vaše ostatní aplikace.

TMF/Gateway není dvojice procesů HP Integrity NonStop Server a je navržena tak, aby se spouštěla v prostředí Pathway. TMF/Gateway vytváří trvalé prostředky v TMF, které přepracuje při následných spuštěních, proto musí TMF/Gateway vždy běžet pod stejným oprávněním uživatele.

Definování třídy serverclass

TMF/Gateway je hostováno jako třída serverclass v prostředí Pathway. Chcete-li definovat třídu serverclass, je třeba nastavit následující atributy serveru:

PROCESSTYPE = OSS

Určuje typ serverů ve třídě serveru. Proces brány je multi-threaded OSS program. Tento atribut je povinný a musí být nastaven na OSS.

MAXSERVERS = 1

Určuje maximální počet procesů serveru v této třídě serveru, které mohou být spuštěny ve stejnou dobu. Pro libovolného správce front může existovat pouze jeden proces brány. Tento atribut je povinný a musí být nastaven na 1.

NUMSTATIC = 1

Určuje maximální počet statických serverů v rámci této třídy serveru. Proces brány musí být spuštěn jako statický server. Tento atribut je povinný a musí být nastaven na 1.

TMF = ON

Uvádí, zda servery v této třídě serveru mohou zamykat a aktualizovat datové soubory, které jsou monitorovány subsystémem TMF. Proces brány se podílí na transakcích TMF aplikací klienta IBM MQ, a proto tento atribut musí být nastaven na ON.

PROGRAM = <OSS installation path>/opt/mqm/bin/runmqtmf

Pro klienta IBM MQ for IBM MQ musí být tento atribut runmqtmf. Tento atribut musí být úplný název OSS cesty. Případ je významný.

ARGLIST = -m < název správce front > [-c < název kanálu >] [-p < port>] [-h < název hostitele >] [-n < max threads>]

Tyto atributy poskytují parametry procesu brány, kde:

- `QMGRName` je název správce front pro tento proces brány. Pokud používáte skupinu sdílení front (nebo jinou technologii rozložení portů), musí být tento parametr zacílen na specifického správce front. Tento parametr je povinný.
- `channel name` je název kanálu serveru ve správci front, který má být používán procesem brány. Tento parametr je volitelný.
- `port` je port protokolu TCP/IP pro správce front. Tento parametr je volitelný.
- `název hostitele` je název hostitele pro správce front. Tento parametr je volitelný.
- `maximální počet podprocesů` je maximální počet pracovních podprocesů vytvořených procesem brány. Tento parametr může nabývat hodnot od 10 výše. Nejnižší hodnota, která se použije, je 10, i když je uvedena hodnota nižší než 10. Není-li zadána žádná hodnota, vytvoří proces brány nejvýše 50 podprocesů.

Použijte atributy `-c`, `-pa` a `-h` jako alternativní způsob poskytování informací o připojení ke komunikační bráně spolu s informacemi popsány v příručce [“Konfigurace TMF/Gateway pomocí proměnných prostředí”](#) na stránce 517. Pokud uvedete jeden nebo více, ale ne všechny atributy `-c`, `-pa` a `-h`, pak atributy, které nezadáte, budou nastaveny jako výchozí hodnoty pro následující hodnoty:

- Výchozí nastavení parametru `název kanálu` je `SYSTEM.DEF.SVRCONN`
- Výchozí hodnota parametru `host name` je `localhost`
- Výchozí hodnota parametru `port` je `1414`.

Je-li některý z parametrů, které jste zadali, neplatný, vydá TMF/Gateway diagnostické zprávy [AMQ5379](#) do protokolu chyb a ukončí se.

OWNER = ID

ID uživatele, pod kterým je spuštěna brána a která musí mít uděleno oprávnění k připojení ke správci front.

SECURITY = "value"

Určuje uživatele ve vztahu k atributu `Owner`, který má přístup k bráně z klientské aplikace IBM MQ.

HIGHPIN = ON

Volitelně určuje, zda proces brány může být spuštěn jako proces s vysokým kolíkem.

CWD = <OSS_install_path>/var/mqm

Určuje pracovní adresář pro proces brány.

`LINKDEPTH` a `MAXLINKS` musí být nakonfigurovány s hodnotami vhodnými pro očekávaný počet klientských aplikací IBM MQ, které mohou chtít souběžně komunikovat s bránou Gateway. Jsou-li tyto hodnoty nastaveny příliš nízké, mohou se zobrazit výskyty chybové zprávy [AMQ5399](#) vydané z klientských aplikací.

Další informace o těchto attributech serveru najdete v příručce *HP NonStop TS/MP 2.5 System Management Manual*.

Konfigurace TMF/Gateway pomocí proměnných prostředí

Jednou z nejběžnějších metod pro definování TMF/Gateway je nastavení proměnné prostředí `MQSERVER`, například:

```
ENV MQSERVER=<channel name>/<transport>/<host name>(<listener port>)
```

ENV na začátku příkazu je notace `Pathway`.

Konfigurace inicializačního souboru klienta

Pokud používáte nástroj HP NonStop Transaction Management Facility (TMF), musíte mít inicializační soubor klienta IBM MQ, abyste umožnili klientovi IBM MQ pro přístup HP Integrity NonStop Server k bráně TMF Gateway.

Inicializační soubor klienta IBM MQ pro HP Integrity NonStop Server lze zadržet v řadě lokalit, abyste získali další informace, viz [“Umístění konfiguračního souboru klienta”](#) na stránce 48.

Podrobné informace o obsahu konfiguračního souboru společně s příkladem viz [“Konfigurace klienta pomocí konfiguračního souboru”](#) na stránce 47. Použijte sekce TMF a TmfGateway k uvedení správce front TMF a podrobnosti o serveru, abyste získali další informace, prohlédněte si téma [“Sekce TMF a TmfGateway”](#) na stránce 71.

Příklad položek pro klienta IBM MQ pro produkt HP Integrity NonStop Server je následující:

```
TMF :  
PathMon=$PSD1P
```

```
TmfGateway :  
QManager=MQ5B  
Server=MQ-MQ5B
```

```
TmfGateway :  
QManager=MQ5C  
Server=MQ-MQ5C
```

Další informace o konfiguraci klienta pomocí proměnných prostředí viz [“Použití proměnných prostředí IBM MQ”](#) na stránce 71.

Udělení oprávnění pro kanály

Udělení oprávnění k kanálům na klientovi IBM MQ pro produkt HP Integrity NonStop Server je stejné jako u jiných operačních systémů, avšak musíte znát identifikaci vlastníka, pod kterým je brána spuštěna.

Pak můžete použít identifikaci vlastníka brány k udělení příslušných oprávnění. Důležitým rozdílem je to, že udělení oprávnění pro kanály správce front není pod oprávněním žádné aplikace.

Pomocí příkazu [setmqaut](#) můžete udělit oprávnění, tj. udělit oprávnění činitele IBM MQ nebo skupině uživatelů oprávnění k provedení operace a k odvolání autorizace, tj. odebrání oprávnění k provedení operace.

V 8.0.0.4 Konfigurace produktu IBM MQ pomocí nástroje Docker

Tyto informace použijte ke konfiguraci produktu IBM MQ pomocí nástroje Docker.

Docker vám umožňuje zabalit správce front IBM MQ nebo aplikaci klienta IBM MQ se všemi jeho závislostmi do standardizované jednotky pro vývoj softwaru.

Změny vaší aplikace mohou být implementovány v testovacím a přechodovém systému rychle a snadno. Tato funkce může být velkým přínosem pro průběžné doručování ve vašem podniku.

V 8.0.0.4 Podpora Docker na systémech Linux

Všimněte si následujících informací, pokud používáte Docker na systému Linux :

- Základní obraz použitý obrazem Docker musí používat operační systém Linux, který je podporován.
- Obraz hostitele, na kterém je spuštěný kontejner Docker, musí používat jádro 3.16 nebo novější jádro Linux a musí se jednat o operační systém podporovaný produktem IBM MQ.
- Chcete-li nainstalovat produkt uvnitř obrazu Docker, musíte použít instalační programy produktu IBM MQ.
- Jsou podporovány pouze následující balíky:
 - MQSeriesRuntime

- MQSeriesServer
 - MQSeriesClient
 - MQSeriesJava
 - MQSeriesJRE
 - MQSeriesGSKit
 - MQSeriesMsg
 - MQSeriesMan
- Datový adresář správce front (standardně /var/mqm) musí být uložen na svazku Docker , který uchovává trvalý stav.

Důležité: Nemůžete používat systém souborů sjednocení.

Musíte buď připojit adresář hostitele jako datový svazek, nebo použít kontejner datového svazku. Další informace naleznete v tématu [Správa dat v kontejnerech](#) .

- Spuštění příkazu `mqconfig` uvnitř kontejneru musí projít, aby bylo zajištěno, že kontejner má správnou konfiguraci.
- Aplikace mohou být lokálně vázány na správce front (režim BINDINGS klienta), jsou-li spuštěny ve stejném kontejneru jako správce front.
- Musíte mít možnost spouštět řídicí příkazy IBM MQ, jako např. `endmqm`, v rámci kontejneru.
- Musíte být schopni získat soubory a adresáře zevnitř kontejneru pro diagnostické účely.

V 8.0.0.4 Plánování vlastního obrazu správce front produktu IBM MQ pomocí nástroje Docker

Tyto informace použijte ke konfiguraci produktu IBM MQ pomocí nástroje Docker. Při spuštění správce front IBM MQ v nástroji Docker je třeba vzít v úvahu několik požadavků. Ukázkový obraz Docker poskytuje způsob zacházení s těmito požadavky, ale pokud chcete použít vlastní obraz, musíte zvážit, jak jsou tyto požadavky obsluhovány.

Řízení procesu

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

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

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

Naplnění /var/mqm

Kontejnery Docker musí být nakonfigurovány s produktem /var/mqm jako svazek Docker .

Provedete-li to, bude adresář svazku při prvním spuštění kontejneru prázdný. Tento adresář je obvykle zaplněn v době instalace, ale instalace a běhová prostředí jsou samostatnými prostředími při použití nástroje Docker.

Chcete-li to vyřešit, až se kontejner spustí, můžete použít příkaz `amqicdir` k naplnění /var/mqm při prvním spuštění.

V 8.0.0.4 Sestavení ukázkového obrazu správce front produktu IBM MQ pomocí nástroje Docker

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

Za prvé, sestavíte základní obraz obsahující systém souborů Ubuntu Linux a čistou instalaci produktu IBM MQ.

Za druhé, sestavíte další vrstvu obrazu Docker na vrcholu báze, která přidá k určité konfiguraci produktu IBM MQ , aby umožnila základní ID uživatele a zabezpečení heslem.

Nakonec spustíte kontejner Docker , který používá tento obraz jako svůj systém souborů, s obsahem adresáře /var/mqm , který je poskytován svazkem Docker specifickým kontejnerem na systému souborů hostitele Docker.

V 8.0.0.4 Sestavení ukázkového obrazu základního správce front produktu IBM MQ

Chcete-li použít produkt IBM MQ v nástroji Docker, musíte nejprve sestavit základní obraz s čistou instalací produktu IBM MQ . Následující kroky ukazují, jak sestavit ukázkový základní obraz, pomocí kódu hostovaného na systému GitHub.

Postup

1. Nainstalujte předem vyžadované balíky.

Tyto pokyny využívají některé balíky produktu Linux , které je třeba instalovat.

- Na Ubuntu:

```
sudo apt-get install python git
```

- V systému Red Hat Enterprise Linux:

```
sudo yum install python git
```

2. Vytvořte adresář `downloads` zadáním příkazu `mkdir downloads`.
3. Stáhněte obraz produktu IBM MQ pro obraz produktu Linux pomocí produktu Passport Advantage.

Další podrobnosti naleznete v tématu [Instalace pomocí elektronického stahování softwaru](#) .

Vyberte například soubor `WS_MQ_V8.0.0.4_LINUX_ON_X86_64_IM.tar.gz` a umístěte soubor do adresáře `downloads` , který jste vytvořili.

4. Zpřístupněte server IBM MQ pro soubor s obrazem Linux (`tar.gz`) na HTTP nebo FTP serveru.

Důvodem je, že se má ušetřit prostor ve vrstvách obrazu Docker . Každá instrukce v souboru Docker způsobí, že bude vytvořena nová vrstva obrazu.

Pokud použijete instrukce **ADD** nebo **COPY** , za nimiž následuje instrukce **RUN** pro instalaci, pak budou soubory přidány nebo zkopírovány do nové vrstvy obrazu potvrzeny.

I když odstraníte soubor v následujících vrstvách, soubor stále existuje v předchozí vrstvě. Z tohoto důvodu je dobrým zvykem stahovat a instalovat v rámci jednoho příkazu **RUN** , což znamená, že soubory musí být dostupné v síti.

Například můžete použít Python ke spuštění serveru HTTP, obsluhující všechny soubory ve vašem aktuálním adresáři:

```
pushd downloads
nohup python -m SimpleHTTPServer 8000 &
popd
```


5. Extrahujte ukázkové soubory pro sestavení podporovaného obrazu Docker z GitHub zadáním následujícího příkazu:

```
git clone -b mq-8 https://github.com/ibm-messaging/mq-docker mq-docker
```

6. Identifikujte vaši IP adresu lokálního systému.

Vaše adresa je specifická pro vaše lokální prostředí, ale měla by být dostupná, pokud spustíte následující příkaz:

```
ip addr show
```

Všimněte si, že localhost nefunguje.

7. Upravte soubor Docker a změňte existující položku pro IBM MQ_URL tak, aby ukazovala na soubor na lokálním souborovém serveru.

Příklad:

```
MQ_URL=http://10.0.2.15:8000/WS_MQ_V8.0.0.4_LINUX_ON_X86_64_IM.tar.gz
```

8. Změňte svůj adresář zadáním následujícího příkazu:

```
cd mq-docker
```

9. Sestavte základní obraz produktu IBM MQ zadáním následujícího příkazu:.

```
sudo docker build --tag mq .
```

Výsledky

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

V 8.0.0.4 Sestavení ukázkového obrazu nakonfigurovaného správce front IBM MQ

Jakmile sestavíte svůj obecný základní obraz produktu IBM MQ Docker , musíte použít vlastní konfiguraci, abyste povolili zabezpečený přístup. Chcete-li to provést, vytvořte vlastní obraz nástroje Docker , který bude používat generický obraz jako nadřazený prvek. Následující kroky ukazují, jak sestavit ukázkový obraz s minimální konfigurací zabezpečení.

Postup

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

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

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

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

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

kde:

- johndoe je ID uživatele, které chcete přidat

- passw0rd je původní heslo

3. Sestavte vlastní obraz Docker pomocí následujícího příkazu:

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

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

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

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

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

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

- Vytvoří správce front.
- Spustí správce front.
- Vytvoří výchozí modul listener.
- Potom spustí jakékoli příkazy MQSC z /etc/mqm/config.mqsc.

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

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

Kde:

První parametr env

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

Další podrobnosti viz [informace o licenci IBM MQ](#) v licencích IBM MQ.

Druhý parametr env

Nastaví název správce front, který používáte.

Parametr svazku

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

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

Parametr publikování

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

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

Parametr odpojení

Spustí kontejner na pozadí.

Výsledky

Zastavili jste nakonfigurovaný obraz nástroje Docker a můžete zobrazit běžící kontejnery pomocí příkazu docker **ps**. Procesy produktu IBM MQ, které jsou spuštěny ve vašem kontejneru, lze zobrazit pomocí příkazu docker **top**.



Upozornění: Pokud se kontejner nezobrazí, když použijete příkaz docker **ps**, kontejner se možná nezdařil. Kontejnery se selháním se zobrazují pomocí příkazu docker **ps -a**.

ID kontejneru se zobrazí pomocí příkazu `docker ps -a` a bylo také vytištěno, když jste zadali příkaz `docker run`.

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

Obecným problémem je to, že `mqconfig` označuje, že některé nastavení jádra na hostiteli Docker nejsou správné. Nastavení jádra jsou sdílena mezi hostitelem a kontejnery Docker a je třeba je nastavit správně (viz [Hardwarové a softwarové požadavky na systémech SYSTÉM UNIX a Linux](#)).

Například, maximální počet otevřených souborů lze nastavit pomocí příkazu `sysctl fs.file-max=524288`.

z/OS

Konfigurace správců front v systému z/OS

Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Před konfigurací produktu IBM MQ si přečtěte informace o koncepcích produktu IBM MQ for z/OS v tématu [Koncepce produktu IBM MQ for z/OS](#).

z/OS Přečtěte si informace o plánování prostředí produktu IBM MQ for z/OS v tématu [Plánování prostředí IBM MQ v systému z/OS](#).

Související pojmy

[“Vytváření a údržba správců front na distribuovaných platformách”](#) na stránce 5

Než budete moci používat zprávy a fronty, musíte vytvořit a spustit alespoň jednoho správce front a jeho přidružené objekty.

[“Konfigurace”](#) na stránce 5

Vytvořte jednoho nebo více správců front na jednom nebo více počítačích a nakonfigurujte je na svých vývojových, testovacích a produkčních systémech a zpracujte zprávy, které obsahují vaše obchodní data.

[“Konfigurace distribuovaných front”](#) na stránce 124

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ, včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

[“Konfigurace připojení mezi serverem a klientem”](#) na stránce 14

Chcete-li nakonfigurovat komunikační propojení mezi IBM MQ MQI clients a servery, rozhodněte se v komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

Související informace

[IBM MQ Technický přehled](#)

[Zabezpečení](#)

[Správa serveru IBM MQ](#)

z/OS [Správa serveru IBM MQ for z/OS](#)

[Naplánování](#)

z/OS [Zadání příkazů](#)

z/OS [Obslužné programy IBM MQ for z/OS](#)

Příprava na přizpůsobení správců front produktu IBM MQ for z/OS

Toto téma vám pomůže při přizpůsobování správců front s podrobnými informacemi o instalovatelných funkcích, národním jazykovým funkcím a informacím o testování a nastavení zabezpečení.

Příprava na přizpůsobení

Programový adresář pro WebSphere MQ pro z/OS vypisuje obsah instalační pásky IBM MQ, informace o programu a servisní úrovni pro IBM MQ a popisuje, jak nainstalovat produkt IBM MQ for z/OS pomocí nástroje SMP/E (System Modification Program Extended).

Pokud jste nainstalovali produkt IBM MQ, musíte provést řadu úloh, než jej budete moci zpřístupnit uživatelům. Popis těchto úloh najdete v následujících částech:

- [“přizpůsobení IBM MQ for z/OS”](#) na stránce 528
- [“Testování správce front v systému z/OS”](#) na stránce 582
- [Nastavení zabezpečení v systému z/OS](#)

Provádíte-li migraci z předchozí verze produktu IBM MQ for z/OS, není třeba provádět většinu úloh přizpůsobení. Další informace o úlohách, které musíte provést, najdete v tématu [Migrace a upgrade produktu IBM MQ](#).

Instalovatelné funkce produktu IBM MQ for z/OS

Produkt IBM MQ for z/OS se skládá z následujících funkcí:

Základ

Tento požadavek je povinný; zahrnuje všechny hlavní funkce, včetně

- Administrace a obslužné programy
- Podpora aplikací CICS, IMSa dávkových typů pomocí rozhraní IBM MQ Application Programming Interface, nebo C++
- Distribuované zařízení řazení do front (podpora komunikace TCP/IP a APPC)

Funkce národního jazyka

Ty obsahují chybové zprávy a panely ve všech podporovaných národních jazycích. Každý jazyk má k sobě přidružený jazykový dopis. Jazyky a písmena jsou:

C

Zjednodušená čínština

E

U.S. angličtina (smíšená velikost písmen)

F

Francouzština

K

japonština

U

U.S. Angličtina (velká písmena)

Musíte nainstalovat volbu americké angličtiny (smíšená velikost písmen). Můžete také instalovat jeden nebo více jiných jazyků. (Proces instalace pro jiné jazyky vyžaduje instalaci americké angličtiny (smíšená velikost písmen), a to i v případě, že nechcete používat americkou angličtinu (smíšená velikost písmen).)

IBM MQ for z/OS Komponenty služeb systému Unix

Tato funkce je volitelná. Vyberte tuto funkci, chcete-li sestavit a spustit aplikace produktu Java, které používají produkt Java Message Service (JMS) pro připojení k produktu IBM MQ for z/OS nebo chcete-li sestavit a spustit aplikace HTTP, které používají protokol HTTP pro připojení k produktu IBM MQ for z/OS.

Knihovny, které existují po instalaci

Produkt IBM MQ je dodáván s řadou samostatných zaváděcích knihoven. [Tabulka 35 na stránce 524](#) zobrazuje knihovny, které mohou existovat až po instalaci produktu IBM MQ.

Název	Popis
thlqual.SCSQANLC	Obsahuje zaváděcí moduly pro zjednodušenou čínskou verzi produktu IBM MQ.

<i>Tabulka 35. Knihovny produktu IBM MQ , které existují po instalaci (pokračování)</i>	
Název	Popis
thlqual.SCSQANLE	Obsahuje zaváděcí moduly pro U.S. Angličtina (smíšená velikost písmen) verze produktu IBM MQ.
thlqual.SCSQANLF	Obsahuje zaváděcí moduly pro francouzskou verzi produktu IBM MQ.
thlqual.SCSQANLK	Obsahuje zaváděcí moduly pro japonskou verzi produktu IBM MQ.
thlqual.SCSQANLU	Obsahuje zaváděcí moduly pro U.S. Anglická (velká) verze produktu IBM MQ.
thlqual.SCSQASMS	Obsahuje zdroj pro ukázkové programy assembleru.
thlqual.SCSQAUTH	Hlavní úložiště pro všechny moduly načtení produktu IBM MQ ; obsahuje také výchozí modul parametrů CSQZPARM. Tato knihovna musí být autorizovaná APF a ve formátu PDS-E.
thlqual.SCSQCICS	Obsahuje další zaváděcí moduly, které musí být zahrnuty do zřetězení CICS DFHRPL. Tato knihovna musí být autorizovaná APF a ve formátu PDS-E.
thlqual.SCSQCLST	Obsahuje CLISTs používané vzorovými programy.
thlqual.SCSQCOBC	Obsahuje zakladače COBOL, včetně zakladačů požadovaných pro ukázkové programy.
thlqual.SCSQCOBS	Obsahuje zdroj ukázkových programů COBOL.
thlqual.SCSQCPPS	Obsahuje zdroj ukázkových programů C + +.
thlqual.SCSQC37S	Obsahuje zdrojový kód pro ukázkové programy C.
thlqual.SCSQC370	Obsahuje záhlaví C, včetně záhlaví požadovaných pro ukázkové programy.
thlqual.SCSQDEFS	Obsahuje definice strany pro C++ a Db2 DBRM pro sdílené řazení do fronty.
thlqual.SCSQEXEC	Obsahuje spustitelné soubory REXX, které mají být zahrnuty do zřetězení SYSEXEC nebo SYSPROC, pokud používáte operační panely a ovládací panely produktu IBM MQ .
thlqual.SCSQHPPS	Obsahuje hlavičkové soubory pro C + +.
thlqual.SCSQINST	Obsahuje JCL pro instalační úlohy.
thlqual.SCSQLINK	Knihovna předčasného kódu. Obsahuje zaváděcí moduly, které jsou načteny při zavedení inicializačního programu systému (IPL). Knihovna musí být autorizovaná APF.
thlqual.SCSQLOAD	Zaveďte knihovnu. Obsahuje zaváděcí moduly pro kód non-APF, uživatelské procedury, obslužné programy, ukázky, programy pro verifikaci instalace a stuby adaptéru. Knihovna nemusí být APF-autorizována a nemusí být ve spojovacím seznamu. Tato knihovna musí být ve formátu PDS-E.
thlqual.SCSQMACS	Obsahuje makra Assembler včetně: ukázková makra, produktová makra a makra parametrů systému.
thlqual.SCSQMAPS	Obsahuje sady CICS mapset používané ukázkovými programy.

<i>Tabulka 35. Knihovny produktu IBM MQ , které existují po instalaci (pokračování)</i>	
Název	Popis
thlqual.SCSQMSGC	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, pokud používáte funkci jazyka Zjednodušená čínština pro operace produktu IBM MQ a řídicí panely.
thlqual.SCSQMSGE	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, používáte-li U.S. Anglická (smíšená) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGF	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, pokud používáte funkci francouzského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGK	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, pokud používáte funkci japonského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGU	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, používáte-li U.S. Anglická (velká) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQMVR1	Obsahuje zaváděcí moduly pro distribuované řazení do fronty. Tato knihovna musí být autorizovaná APF a ve formátu PDS-E.
thlqual.SCSQPLIC	Obsahuje soubory začlenění PL/I.
thlqual.SCSQPLIS	Obsahuje zdroj ukázkových programů PL/I.
thlqual.SCSQPMLA	Obsahuje panely IPCS, pro formátovač výpisů paměti, které mají být zahrnuty do zřetězení ISPPLIB. Obsahuje také panely s ukázkovými programy produktu IBM MQ .
thlqual.SCSQPMLC	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, pokud používáte funkci jazyka Zjednodušená čínština pro operace produktu IBM MQ a ovládací panely.
thlqual.SCSQPMLE	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, používáte-li U.S. Anglická (smíšená) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQPMLF	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení souboru ISPPLIB, pokud používáte funkci francouzského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQPMLK	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, pokud používáte funkci japonského jazyka pro operace produktu IBM MQ a ovládací panely.
thlqual.SCSQPMLU	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, používáte-li U.S. Anglická (velká) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQPROC	Obsahuje ukázkové datové sady JCL a výchozí inicializační datové sady systému.
thlqual.SCSQSNLC	Obsahuje zaváděcí moduly pro zjednodušenou čínskou verzi modulů IBM MQ , které jsou vyžadovány pro funkci speciálního účelu (například pro počáteční kód).

<i>Tabulka 35. Knihovny produktu IBM MQ , které existují po instalaci (pokračování)</i>	
Název	Popis
thlqual.SCSQSNLE	Obsahuje zaváděcí moduly pro U.S. Anglická (směs malých a velkých písmen) modulů IBM MQ , které jsou vyžadovány pro speciální účel (například včasný kód).
thlqual.SCSQSNLF	Obsahuje zaváděcí moduly pro francouzské verze modulů IBM MQ , které jsou vyžadovány pro speciální účelovou funkci (například na začátku kódu).
thlqual.SCSQSNLK	Obsahuje zaváděcí moduly pro japonské verze modulů IBM MQ , které jsou vyžadovány pro speciální účelovou funkci (například na začátku kódu).
thlqual.SCSQSNLU	Obsahuje zaváděcí moduly pro U.S. Anglická (velká) verze modulů IBM MQ , které jsou vyžadovány pro funkci speciálního účelu (například včasný kód).
thlqual.SCSQTBLC	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, pokud používáte funkci jazyka Zjednodušená čínština pro operace produktu IBM MQ a řídicí panely.
thlqual.SCSQTBLE	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, používáte-li U.S. Anglická (smíšená) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQTBLF	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, pokud používáte funkci francouzského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQTBLK	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, pokud používáte funkci japonského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQTBLU	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, používáte-li U.S. Anglická (velká) jazyková funkce pro operace IBM MQ a ovládací panely.

Poznámka: Neupravujte ani neupravujte žádnou z těchto knihoven. Chcete-li provést změny, zkopírujte knihovny a proveďte změny na jejich kopii.

Související pojmy

“Nastavení komunikace s ostatními správci front” na stránce 590

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS , které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

“Použití IBM MQ s IMS” na stránce 619

Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

“Použití IBM MQ s CICS” na stránce 627

Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge .

“Použití uživatelských procedur OTMA v produktu IMS” na stránce 630

Toto téma použijte v případě, že chcete použít uživatelské procedury IMS Open Transaction Manager Access s IBM MQ for z/OS.

Související odkazy

“Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services” na stránce 627

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

Související informace

[IBM MQ for z/OS koncepce](#)

[Správa serveru IBM MQ for z/OS](#)

přizpůsobení IBM MQ for z/OS

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ .

Toto téma vás provede různými fázemi přizpůsobení IBM MQ poté, co jste jej úspěšně nainstalovali. Proces instalace je popsán v adresáři programu, který je k dispozici ke stažení na webu [IBM Publications Center](#).

Ukázky jsou dodávány s produktem IBM MQ , aby vám pomohly s přizpůsobením. Členové ukázkových datových sad mají názvy začínající na čtyři znaky CSQ4 a jsou v knihovně thlqual.SCSQPROC.

Než provedete úlohy přizpůsobení popsané v tomto tématu, je zde řada voleb konfigurace, které musíte zvážit, protože ovlivňují výkon a požadavky na prostředky produktu IBM MQ for z/OS. Musíte se například rozhodnout, které knihovny globalizace chcete použít.

Volby konfigurace

Další informace o těchto volbách viz [Plánování v systému z/OS](#).

Popis každé úlohy v této sekci označuje, zda:

- Úloha je součástí procesu přizpůsobení IBM MQ. To znamená, že provedete úlohu jednou, když upravíte IBM MQ na systému z/OS . (V paralelním prostředí sysplex musíte provést úlohu pro každý systém z/OS v prostředí sysplex a ujistěte se, že každý systém z/OS je nastaven stejně.)
- Úloha je součástí přidání správce front. To znamená, že provedete úlohu jednou pro každého správce front, když přidáte tohoto správce front.
- Je třeba provést úlohu při migraci. Migrujete-li z předchozí verze produktu IBM MQ for z/OS, nemusíte provádět všechny tyto úlohy.

Přezkoumejte úlohy, když použijete opravnou údržbu na IBM MQ a když instalujete novou verzi nebo vydání IBM MQ.

Žádná z úloh nevyžaduje, abyste provedli IPL systému z/OS , pokud používáte příkazy ke změně různých systémových parametrů z/OS , a proveďte [“Úloha 12: Aktualizace SYS1.PARMLIB členové”](#) na stránce 544 jak je doporučeno.

Chcete-li zjednodušit operace a usnadnit určování problémů, ujistěte se, že všechny systémy z/OS v prostředí sysplex jsou nastaveny stejně, takže správci front mohou být rychle vytvořeni na libovolném systému v nouzi.

Kvůli usnadnění údržby zvažte definování aliasů tak, aby odkazovaly na knihovny produktu IBM MQ ; další informace naleznete v tématu [Použití aliasu pro odkaz na knihovnu IBM MQ](#).

Identifikovat knihovny národní jazykové podpory

Musíte uvést příslušné knihovny globalizace v souboru JCL, které chcete použít s produktem IBM MQ (jak je popsáno v následujících oddílech). Každý jazyk je identifikován pomocí jazykového dopisu:

C

Zjednodušená čínština

E

U.S. angličtina (smíšená velikost písmen)

F

Francouzština

K

japonština

U

U.S. Angličtina (velká písmena)

Tabulka 36. Knihovny funkcí národních jazyků

Popis	japonština	Zjednodušená čínština	U.S. angličtina (smíšená velikost písmen)	U.S. Angličtina (velká písmena)	Francouzština
Zaváděcí moduly	thlqual.SCSQAN LK	thlqual.SCSQAN LC	thlqual.SCSQAN LE	thlqual.SCSQAN LU	thlqual.SCSQAN LF
Zprávy ISPF	thlqual.SCSQMS GK	thlqual.SCSQMS GC	thlqual.SCSQMS GE	thlqual.SCSQMS GU	thlqual.SCSQMS GF
Panely ISPF	thlqual.SCSQPN LK	thlqual.SCSQPN LC	thlqual.SCSQPN LE	thlqual.SCSQPN LU	thlqual.SCSQPN LF
Speciální účelová funkce (například dřívější kód)	thlqual.SCSQSN LK	thlqual.SCSQSN LC	thlqual.SCSQSN LE	thlqual.SCSQSN LU	thlqual.SCSQSN LF
Tabulky ISPF	thlqual.SCSQTBL K	thlqual.SCSQTBL C	thlqual.SCSQTBL E	thlqual.SCSQTBL U	thlqual.SCSQTBL F

Souhrn přizpůsobení

V následující tabulce jsou uvedeny všechny kroky, které je třeba provést při přizpůsobení produktu IBM MQ for z/OS. Také označuje následující:

- Zda má být krok proveden pouze jednou, nebo se opakuje pro každého správce front.
- Zda se má opakovat krok pro každou skupinu sdílení front, nebo tento krok vynechat, pokud nepoužíváte skupiny sdílení front.
- Určuje, zda je krok nezbytný, pokud provádíte migraci z předchozí verze produktu IBM MQ. Některé kroky mohou být potřebné v závislosti na tom, co se rozhodnete pro názvy datové sady a správce front; tyto kroky jsou označeny jako 'Revize'.

Tabulka 37. Souhrn přizpůsobení

Úloha	Nezbytné při migraci	Opakovat pro každého správce front	Skupiny sdílení front
“Úloha 1: Identifikovat parametry systému z/OS” na stránce 531	Revize	-	-
“Úloha 2: Autorizace APF pro zaváděcí knihovny produktu IBM MQ” na stránce 532	Revize	-	-
“Úloha 3: Aktualizace seznamu odkazů z/OS a LPA” na stránce 532	Revize	-	-
“Úloha 4: Aktualizace tabulky vlastností programu z/OS” na stránce 534	-	-	-
“Úloha 5: Definujte subsystém IBM MQ na z/OS” na stránce 534	-	X	-
“Úloha 6: Vytvořit procedury pro správce front IBM MQ” na stránce 538	Revize	X	-

<i>Tabulka 37. Souhrn přizpůsobení (pokračování)</i>			
Úloha	Nezbytné při migraci	Opakovat pro každého správce front	Skupiny sdílení front
“Úloha 7: Vytvořit procedury pro inicializátor kanálu” na stránce 539	Revize	X	-
“Úloha 8: Definování subsystému IBM MQ pro třídu služeb z/OS WLM” na stránce 540	-	X	-
“Úloha 9: Nastavení prostředí Db2” na stránce 541	Revize	-	Vynechat, pokud se nepoužívá
“Úloha 10: Nastavení prostředku Coupling Facility” na stránce 542	Revize	-	Opakovat pro každý
“Úloha 11: Implementovat ovládací prvky zabezpečení ESM” na stránce 543	Revize	X	X
“Úloha 12: Aktualizace SYS1.PARMLIB členové” na stránce 544	Revize	-	-
“Úloha 13: Úprava vstupních datových sad inicializace” na stránce 545	X	X	-
“Úloha 14: Vytvoření zaváděcího programu a datových sad protokolu” na stránce 548	-	X	-
“Úloha 15: Definujte sady stránek” na stránce 549	-	X	-
“Úloha 16: Přidání položek IBM MQ do tabulek Db2” na stránce 549	Revize	X	Opakovat pro každý
“Úloha 17: Přizpůsobte modul parametrů systému” na stránce 550	X	X	-
“Úloha 18: Přizpůsobte parametry inicializátoru kanálu” na stránce 572	X	X	-
“Úloha 19: Nastavení dávky, TSO a adaptérů RRS” na stránce 574	Revize	-	-
“Úloha 20: Nastavení panelů operací a ovládacích panelů” na stránce 574	Revize	-	-
“Úloha 21: Zahrnout členu formátování výpisu paměti IBM MQ” na stránce 576	X	-	-
“Úloha 22: Potlačit informační zprávy” na stránce 576	-	-	-
“Úloha 23: Vytvořit procedury pro rozšířené zabezpečení zpráv” na stránce 577	Revize	X	-
“Úloha 24: Nastavit zabezpečení rozšířených zpráv spuštěné úlohy uživatele” na stránce 578	Revize	X	-
“Úloha 25: Udělení oprávnění RACDCERT správci zabezpečení pro rozšířenou bezpečnost zpráv” na stránce 580	-	-	-

Tabulka 37. Souhrn přízpůsobení (pokračování)

Úloha	Nezbytné při migraci	Opakovat pro každého správce front	Skupiny sdílení front
“Úloha 26: Udělení oprávnění k prostředkům uživatelům pro produkt IBM MQ Advanced Message Security” na stránce 581	-	-	-

Související pojmy

“Nastavení komunikace s ostatními správci front” na stránce 590

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS , které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

“Použití IBM MQ s IMS” na stránce 619

Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

“Použití IBM MQ s CICS” na stránce 627

Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge .

“Použití uživatelských procedur OTMA v produktu IMS” na stránce 630

Toto téma použijte v případě, že chcete použít uživatelské procedury IMS Open Transaction Manager Access s IBM MQ for z/OS.

Související odkazy

“Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services” na stránce 627

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

Související informace

[IBM MQ for z/OS koncepce](#)

[Správa serveru IBM MQ for z/OS](#)

[Programový adresář pro IBM MQ for z/OS](#)

Úloha 1: Identifikovat parametry systému z/OS

Některé z úloh zahrnují aktualizaci systémových parametrů produktu z/OS . Musíte vědět, které z nich byly zadány při provádění IPL systému.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

SYS1.PARMLIB(IEASYSpp) obsahuje seznam parametrů, které odkazují na jiné členy SYS1.PARMLIB (kde pp představuje seznam parametrů systému z/OS , který byl použit k provedení IPL systému).

Položky, které potřebujete najít, jsou:

Pro “Úloha 2: Autorizace APF pro zaváděcí knihovny produktu IBM MQ” na stránce 532:

PROG=xx nebo APF=aa, aby ukazovala na seznam autorizovaných knihoven APF (Authorized Program Facility) (člen PROGxx nebo IEFAPFaa)

Pro “Úloha 3: Aktualizace seznamu odkazů z/OS a LPA” na stránce 532:

LNK=kk ukazuje na seznam propojení (člen LNKLSTkk) LPA=mm ukazuje na seznam LPA (člen LPALSTmm)

Pro “Úloha 4: Aktualizace tabulky vlastností programu z/OS” na stránce 534:

SCH=xx ukazuje na tabulku vlastností programu (PPT) (člen SCHEDxx)

Pro “Úloha 5: Definujte subsystém IBM MQ na z/OS” na stránce 534:

SSN=ss ukazuje na definovaný seznam subsystémů (člen IEFSSNss)

Úloha 2: Autorizace APF pro zaváděcí knihovny produktu IBM MQ

APF-autorizovat různé knihovny. Některé zaváděcí moduly již mohou být autorizovány.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že jsou nastavení pro IBM MQ identická na každém systému z/OS v prostředí sysplex.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Zaváděcí knihovny IBM MQ thlqual.SCSQAUTH a thlqual.SCSQLINK musí mít oprávnění APF-. Musíte také APF autorizovat knihovny pro funkce národního jazyka (thlqual.SCSQANLx a thlqual.SCSQSNLx) a pro funkce distribuovaných front (thlqual.SCSQMVR1). Pokud používáte IBM MQ Advanced Message Security , musíte také autorizovat APF pro knihovnu thlqual.SDRQAUTH.

Nicméně všechny zaváděcí moduly v LPA jsou automaticky autorizovány APF. Jsou-li tedy SYS1.PARMLIB člen IEASYSpp obsahuje následující příkaz:

```
LNKAUTH=LNKLST
```

LNKAUTH=LNKLST je předvolba, pokud není uvedeno LNKAUTH.

V závislosti na tom, co vyberete pro vložení do LPA nebo seznamu odkazů (viz “[Úloha 3: Aktualizace seznamu odkazů z/OS a LPA](#)” na stránce 532), možná nebudete muset umístit knihovny do seznamu odkazů APF

Poznámka: Musíte APF autorizovat všechny knihovny, které zahrnete do STEPLIB produktu IBM MQ . Pokud vložíte do STEPLIB knihovnu, která není autorizována APF, ztratí zřetězení knihovny autorizaci APF.

Seznamy APF jsou v SYS1.PARMLIB member PROGxx nebo IEAAPFaa. Seznamy obsahují názvy autorizovaných knihoven z/OS APF. Pořadí položek v seznamech není významné. Informace o seznamech APF najdete v příručce *MVS Initialization and Tuning Reference* .

Další informace o ladění systému najdete v tématu [SupportPac MP16](#) .

Pokud použijete členy PROGxx s dynamickým formátem, musíte vydat pouze příkaz z/OS SETPROG APF , ADD , DSNAME=h1q . SCSQ XXXX , VOLUME= YYYYYY , aby se změny projevíly: Kde XXXX se liší podle názvu knihovny a kde YYYYYY je hlasitost. Jinak, pokud používáte statický formát nebo IEAPFaa členy, musíte provést IPL na systému.

Všimněte si, že musíte použít skutečný název knihovny v seznamu APF. Pokusíte-li se použít alias datové sady knihovny, autorizace selže.

Související pojmy

“[Úloha 3: Aktualizace seznamu odkazů z/OS a LPA](#)” na stránce 532

Aktualizujte knihovny LPA pomocí nové verze knihoven s časným kódem. Ostatní kódy mohou být uvedeny v seznamu odkazů nebo v oblasti LPA.

“[Příprava na přizpůsobení správců front produktu IBM MQ for z/OS](#)” na stránce 523

Toto téma vám pomůže při přizpůsobování správců front s podrobnými informacemi o instalovatelných funkcích, národním jazykovým funkcím a informacím o testování a nastavení zabezpečení.

Úloha 3: Aktualizace seznamu odkazů z/OS a LPA

Aktualizujte knihovny LPA pomocí nové verze knihoven s časným kódem. Ostatní kódy mohou být uvedeny v seznamu odkazů nebo v oblasti LPA.

- Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.
- Pokud používáte skupiny sdílení front, musíte se ujistit, že jsou nastavení pro IBM MQ identická na každém systému z/OS v prostředí sysplex.

- Možná budete muset provést tuto úlohu při migraci z předchozí verze. Podrobnosti naleznete v příručce [Programový adresář pro WebSphere MQ pro z/OS](#).

Poznámka: Datová sada pro LPA je specifická pro verzi. Pokud používáte existující LPA v systému, obraťte se na administrátora systému, aby rozhodl, který server LPA se má použít.

Předčasný kód

Některé zaváděcí moduly produktu IBM MQ je třeba přidat do systému MVS pro příkaz IBM MQ , aby se choval jako subsystém. Tyto moduly jsou známy jako úvodní kód a lze je spouštět i v případě, že správce front není aktivní. Je-li například na konzole zadán příkaz operátora s předponou příkazu IBM MQ , tento Early kód získá kontrolu a zkontroluje, zda potřebuje spustit správce front, nebo předat požadavek spuštěnému správcí front. Tento kód je načten do oblasti LPA (Link Pack Area). Existuje jedna sada Early modulů, které se používají pro všechny správce front, a ty je třeba mít na nejvyšší úrovni IBM MQ. Early code from a higher version of IBM MQ will work with a queue manager with a lower version of IBM MQ, but not the opposite.

IBM MQ

První kód se skládá z následujících modulů zatížení:

- CSQ3INI a CSQ3EPX v knihovně thqual.SCSQLINK
- CSQ3ECMX v knihovně thqual.SCSQSNL x, kde x je váš jazykový dopis.

Produkt IBM MQ zahrnuje úpravu uživatele, která přesouvá obsah knihovny thqual.SCSQSNL x do souboru thqual.SCSQLINK a informuje SMP/E. Tato změna uživatele se nazývá CSQ8UERL a je popsána v publikaci [Programový adresář pro WebSphere MQ pro z/OS](#).

When you have updated the early code in the LPA libraries, it is available from the next z/OS IPL (with the CLPA option) to all queue manager subsystems added during IPL from definitions in IEFSSNss members in SYS1.PARMLIB.

Můžete ji zpřístupnit okamžitě bez provedení IPL pro každý nový subsystém správce front přidáný později (jak je popsáno v tématu [“Úloha 5: Definujte subsystém IBM MQ na z/OS”](#) na stránce 534). přidáním do LPA takto:

- Pokud jste nepoužili CSQ8UERL, zadejte tyto příkazy z/OS :

```
SETPROG LPA,ADD,MODNAME=(CSQ3INI,CSQ3EPX),DSNAME=thqual.SCSQLINK
SETPROG LPA,ADD,MODNAME=(CSQ3ECMX),DSNAME=thqual.SCSQSNL x
```

- Pokud jste použili CSQ8UERL, můžete do LPA načíst počáteční kód pomocí následujícího příkazu z/OS :

```
SETPROG LPA,ADD,MASK=*,DSNAME=thqual.SCSQLINK
```

- Pokud používáte IBM MQ Advanced Message Security , musíte také vydat následující příkaz z/OS , aby zahrnoval další modul v LPA:

```
SETPROG LPA,ADD,MODNAME=(CSQ0DRTM),DSNAME=thqual.SCSQLINK
```

Pokud jste použili údržbu nebo chcete restartovat správce front s novější verzí nebo verzí produktu IBM MQ, může být dřívější kód zpřístupněn pro subsystémy správce front, které jsou již definovány. Chcete-li jej zpřístupnit, použijte následující kroky:

1. Přidejte jej do LPA pomocí příkazů z/OS SETPROG, jak je popsáno výše v tomto tématu.
2. Zastavte správce front pomocí příkazu IBM MQ STOP QMGR.
3. Ujistěte se, že qmgr.REFRESH.QMGR je nastaven. Viz [příkazy MQSC, profily a jejich úrovně přístupu](#).
4. Aktualizujte počáteční kód pro správce front pomocí příkazu IBM MQ REFRESH QMGR TYPE (EARLY).
5. Restartujte správce front pomocí příkazu IBM MQ START QMGR.

Příkazy IBM MQ STOP QMGR, REFRESH QMGR a START QMGR jsou popsány v [příkazech MQSC](#).

Jiný kód

Všechny zaváděcí moduly dodané IBM MQ v následujících knihovnách jsou reentrantní a lze je umístit do LPA:

- SCSQAUTH
- SCSQANL *x*, kde *x* je váš jazykový dopis
- SCSQMVR1

Důležité: Pokud však umístíte knihovny do LPA, kdykoli použijete údržbu, budete muset ručně okopírovat všechny změněné moduly do LPA. Proto je vhodnější umístit zaváděcí knihovny produktu IBM MQ do seznamu odkazů, které lze aktualizovat po údržbě zadáním příkazu z/OS REFRESH LLA.

To je zvláště doporučeno pro SCSQAUTH, takže je nemusíte zahrnout do několika STEPLIBs. Pouze jedna jazyková knihovna, SCSQANL *x* by měla být umístěna v seznamu LPA nebo seznamu odkazů. Knihovny seznamu odkazů jsou uvedeny v členu LNKLSTkk členu SYS1.PARMLIB.

Distribuované zařízení pro práci s frontami a produkt CICS bridge (nikoli však samotný správce front) potřebují přístup ke knihovně běhových prostředí SCEERUN běhového prostředí jazyka LE (Language Environment). Pokud použijete kterýkoli z těchto zařízení, musíte zahrnout SCEERUN do seznamu odkazů.

Související pojmy

[“Úloha 4: Aktualizace tabulky vlastností programu z/OS”](#) na stránce 534

Pro správce front produktu IBM MQ jsou zapotřebí některé další položky PPT.

Úloha 4: Aktualizace tabulky vlastností programu z/OS

Pro správce front produktu IBM MQ jsou zapotřebí některé další položky PPT.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS, na kterém chcete spustit produkt IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že jsou nastavení pro IBM MQ identická na každém systému z/OS v prostředí sysplex.*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*
- *Chcete-li vyžadovat produkt IBM MQ Advanced Message Security, musíte provést část CSQ0DSRV této úlohy.*

Ukázka obsahující všechny požadované položky PPT je poskytnuta v souboru thlqual.SCSQPROC(CSQ4SCHED). Ujistěte se, že jsou požadované záznamy přidány do PPT, které můžete najít v SYS1.PARMLIB(SCHEDxx).

V produktu z/OS 1.12 a v novějších verzích je CSQYASCP již definován pro operační systém s atributy detailními a již nemusí být zahrnuti do členu SCHEDxx oblasti PARMLIB.

Správce front produktu IBM MQ řídí výměnu sebe sama. Pokud však máte silně zatížené IBM MQ sítě a doba odezvy je kritická, může být výhodné nastavit iniciátor kanálu IBM MQ nespojovatelým přidáním položky CSQXJST PPT, a to s rizikem ovlivnění výkonu zbytku vašeho systému z/OS.

Požadujete-li IBM MQ Advanced Message Security, přidejte položku PPT CSQ0DSRV.

Vydejte příkaz z/OS SET SCH=, aby se tyto změny projevíly.

Související pojmy

[“Úloha 5: Definujte subsystém IBM MQ na z/OS”](#) na stránce 534

Aktualizujte tabulku názvů subsystémů a rozhodněte se podle konvence pro řetězce předpony příkazu.

Úloha 5: Definujte subsystém IBM MQ na z/OS

Aktualizujte tabulku názvů subsystémů a rozhodněte se podle konvence pro řetězce předpony příkazu.

Opakujte tuto úlohu pro každého správce front produktu IBM MQ. Při migraci z předchozí verze není třeba tuto úlohu provést.

Související pojmy

“Úloha 6: Vytvořit procedury pro správce front IBM MQ” na stránce 538

Každý subsystém IBM MQ potřebuje katalogovou proceduru ke spuštění správce front. Můžete vytvořit vlastní nebo použít knihovnu procedur dodané s produktem IBM.

Aktualizace tabulky názvů subsystémů

Při definování subsystému IBM MQ je třeba přidat položku do tabulky názvů subsystémů.

Tabulka názvů subsystémů produktu z/OS, která je původně brána z SYS1.PARMLIB člen IEFSSNss, obsahuje definice formálně definovaných subsystémů z/OS . Chcete-li definovat každý subsystém IBM MQ , musíte do této tabulky přidat položku, a to buď změnou člena IEFSSNss SYS1.PARMLIB, nebo pokud možno, pomocí příkazu z/OS SETSSI.

Inicializace subsystému IBM MQ podporuje paralelní zpracování, takže lze do tabulky IEFSSNss v tabulce IEFSSNss, která je k dispozici na serveru z/OS V1.12 , a později, přidat příkazy definice subsystému IBM MQ , a to jak nad a pod klíčovým slovem BEGINPARALLEL.

Použijete-li příkaz SETSSI, změna se projeví okamžitě a není třeba provádět IPL systému. Ujistěte se, že aktualizujete SYS1.PARMLIB stejně tak, jak je popsáno v tématu “Úloha 12: Aktualizace SYS1.PARMLIB členové” na stránce 544 , takže změny zůstávají v platnosti po následných IPL.

Příkaz SETSSI pro dynamické definování subsystému IBM MQ je následující:

```
SETSSI ADD,S=ssid,I=CSQ3INI,P='CSQ3EPX,cpf,scope'
```

Odpovídající informace v IEFSSNss lze zadat jedním ze dvou způsobů:

- Formát parametru klíčového slova v definici subsystému IBM MQ v IEFSSNss. Toto je doporučená metoda.

```
SUBSYS SUBNAME(ssid) INITRTN(CSQ3INI) INITPARM('CSQ3EPX,cpf,scope')
```

- Poziční parametr z definice subsystému IBM MQ .

```
ssid,CSQ3INI,'CSQ3EPX,cpf,scope'
```

Nesměšujte tyto dva formuláře v jednom členu IEFSSNss. Pokud jsou vyžadovány různé formuláře, použijte oddělený člen IEFSSNss pro každý typ, přidáním operandu SSN nového člena do IEASYSpp SYS1.PARMLIB . Chcete-li určit více než jednu společnost SSN, použijte společnost SSN = (aa, bb, ...) v IEASYSpp.

V příkladech:

ssid

Identifikátor subsystému. Může mít délku až čtyři znaky. Všechny znaky musí být alfanumerické (velká písmena A až Z, 0 až 9), musí začínat abecedním znakem. Správce front bude mít stejný název jako subsystém, a proto můžete použít pouze znaky, které jsou povoleny pro názvy subsystémů z/OS i názvy objektů produktu IBM MQ .

cpf

Řetězec předpony příkazu (informace o CPF naleznete v příručce “Definování řetězců s předponou příkazu (CPF)” na stránce 536).

scope

Rozsah systému, použitý, pokud pracujete v prostředí sysplex z/OS (informace o rozsahu systému viz “Kódy CPF v prostředí sysplex” na stránce 537).

Příkaz Obrázek 90 na stránce 536 zobrazuje několik příkladů příkazů IEFSSNss.

```
CSQ1,CSQ3INI,'CSQ3EPX,+mqs1cpf,S'
CSQ2,CSQ3INI,'CSQ3EPX,+mqs2cpf,S'
CSQ3,CSQ3INI,'CSQ3EPX,++,S'
```

Obrázek 90. Ukázka příkazů IEFSSNss pro definování subsystémů

Poznámka: Pokud jste v subsystému vytvořili objekty, nemůžete změnit název subsystému nebo použít sady stránek z jednoho subsystému v jiném subsystému. Chcete-li provést některou z těchto úloh, je nutné uvolnit všechny objekty a zprávy z jednoho subsystému a znovu je načíst do jiného subsystému.

Tabulka 38 na stránce 536 udává počet příkladů, které zobrazují přidružení názvů subsystémů a řetězců s předponou příkazu, jak je definováno příkazy v [Obrázek 90 na stránce 536](#).

Tabulka 38. Název subsystému pro přidružení CPF	
Název podsystému IBM MQ	CPF
CSQ1	+mqs1cpf
CSQ2	+mqs2cpf
CSQ3	++

Poznámka: Funkce ACTIVATE a DEACTIVATE příkazu z/OS SETSSI nejsou podporovány produktem IBM MQ.

Chcete-li zkontrolovat stav těchto změn, zadejte následující příkaz v SDSF: /D SSI , L. Zobrazí se nové subsystémy vytvořené ve stavu AKTIVNÍ.

Definování řetězců s předponou příkazu (CPF)

Každá instance subsystému IBM MQ může mít řetězec předpony příkazu k identifikaci tohoto subsystému.

Převzetí celosystémové konvence pro vaše CPF pro všechny subsystémy, aby nedocházelo ke konfliktům. Dodržují pokyny k následujícím pokynům:

- Definujte CPF jako řetězec o délce až osmi znaků.
- Nepoužívejte CPF, který je již používán jiným podsystémem, a vyvarujte se použití znaku backspace JES definovaného ve vašem systému jako prvního znaku vašeho řetězce.
- Definujte CPF pomocí znaků ze sady platných znaků vypsanych v [Tabulka 40 na stránce 537](#).
- Nepoužívejte CPF, který je zkratka pro již definovaný proces, nebo který může být zaměňován s syntaxí příkazu. Například, CPF jako 'D' conflicts with z/OS commands such as ' DISPLAY. Chcete-li se tomuto problému vyhnout, použijte jeden ze speciálních znaků (viz [Tabulka 40 na stránce 537](#)). jako první nebo jediný znak v řetězci CPF.
- Nedefinujte CPF, který je buď podmnožinou, nebo nadřazenou sadou existujícího CPF. Příklad viz [Tabulka 39 na stránce 536](#).

Tabulka 39. Příklad dílčí sady CPF a pravidel supersady

Název podsystému	Definované CPF	Příkazy směřované do
MQA	!A	MQA
MQB	!B	MQB
MQC1	!C1	MQC1
MQC2	!C2	MQC2
MQB1	!B1	MQB

Příkazy určené pro subsystém MQB1 (použití CPF!)B1) jsou směřovány do subsystému MQB, protože CPF pro tento subsystém je!B, podmnožina!B1. Pokud jste například zadali příkaz:

```
!B1 START QMGR
```

Subsystém MQB přijímá příkaz:

```
1 START QMGR
```

(který se v tomto případě nemůže vypořádat s).

Chcete-li zjistit, které předpony existují, zadejte příkaz z/OS DISPLAY OPDATA.

Pokud pracujete v prostředí sysplex, produkt z/OS diagnostikuje všechny konflikty tohoto typu v době registrace CPF (viz [“Kódy CPF v prostředí sysplex”](#) na stránce 537, kde získáte informace o registraci CPF).

Tabulka 40 na stránce 537 ukazuje znaky, které můžete použít při definování řetězců CPF:

<i>Tabulka 40. Platná znaková sada pro řetězce CPF</i>	
Znaková sada	Obsah
Abecední	velká písmena A až Z, malá a až z
Číselné	0 až 9
Národní (viz poznámka)	@ \$# (znaky, které mohou být reprezentovány jako hexadecimální hodnoty)
Speciální	. □ () * & + - = ¢ < ! ; % _ ? : >

Poznámka:

Systém rozpoznává následující hexadecimální reprezentace národních znaků: @ jako X'7C', \$ jako X'5B' a # jako X'7B'. V jiných zemích, než je U.S. U.S. Národní znaky znázorněné na klávesnicích terminálu mohou generovat jinou hexadecimální reprezentaci a způsobit chybu. Například v některých zemích může znak \$generovat symbol '4A'.

Středník (;) je platný jako CPF, ale ve většině systémů tento znak je oddělovač příkazů.

Kódy CPF v prostředí sysplex

Toto téma vám pomůže porozumět způsobu použití rozhraní CPF v rámci oboru prostředí sysplex.

Pokud se používá v prostředí sysplex, IBM MQ registruje vaše CPF, aby vám umožnil zadat příkaz z libovolné konzoly v prostředí sysplex a směřovat tento příkaz na vhodný systém pro provedení. Odezvy příkazu se vrátí na původní konzolu.

Definování rozsahu pro operaci prostředí sysplex

Rozsah se používá k určení typu registrace CPF prováděné subsystémem IBM MQ, když provozujete produkt IBM MQ v prostředí sysplex.

Možné hodnoty rozsahu jsou následující:

M

Rozsah systému.

CPF je registrován s z/OS v době IPL systému produktem IBM MQ a zůstává registrován pro celou dobu, kdy je systém z/OS aktivní.

Příkazy IBM MQ musí být zadávány na konzole připojené k obrazu z/OS, kde je spuštěn cílový subsystém, nebo musíte použít příkazy ROUTE pro přesměrování příkazu na tento obraz.

Tuto volbu použijte, pokud není spuštěna v prostředí sysplex.

S

Byl spuštěn rozsah prostředí sysplex.

CPF je registrován u z/OS při spuštění podsystému IBM MQ a zůstává aktivní, dokud se subsystém IBM MQ neukončí.

Chcete-li směřovat původní příkaz START QMGR na cílový systém, musíte použít příkazy ROUTE, ale všechny další příkazy IBM MQ lze zadat na libovolné konzoli připojené k prostředí sysplex a jsou směřovány do cílového systému automaticky.

Po ukončení IBM MQ musíte použít příkazy ROUTE pro směrování následných příkazů START do cílového subsystému IBM MQ .

X

Rozsah IPL prostředí sysplex.

CPF je registrován s z/OS v době IPL systému produktem IBM MQ a zůstává registrován pro celou dobu, kdy je systém z/OS aktivní.

Příkazy IBM MQ lze zadat na libovolné konzoli připojené k prostředí sysplex a jsou směřovány na obraz, který automaticky provádí cílový systém.

Subsystém IBM MQ s rozsahem CPF s rozsahem S může být definován na jednom nebo více obrazech z/OS v prostředí sysplex, takže tyto obrazy mohou sdílet jednu tabulku názvů subsystémů. Musíte však zajistit, aby počáteční příkaz START byl zadán (nebo přesměrován na) obraz z/OS , na kterém má být spuštěn subsystém IBM MQ . Použijete-li tuto volbu, můžete zastavit subsystém IBM MQ a restartovat jej na jiném obraze produktu z/OS v rámci prostředí sysplex, aniž byste museli měnit tabulku názvů subsystémů nebo provádět IPL systému z/OS .

Subsystém IBM MQ s rozsahem CPF s rozsahem X může být definován pouze na jednom obraze z/OS v rámci prostředí sysplex. Použijete-li tuto volbu, musíte definovat jedinečnou tabulku názvů subsystémů pro každý obraz produktu z/OS , který vyžaduje IBM MQ subsystémů s hodnotami CPF rozsahu X.

Chcete-li správce automatického restartu produktu z/OS (ARM) použít k automatickému restartování správců front v různých obrazech produktu z/OS , musí být každý správce front definován v každém obraze produktu z/OS , na kterém může být správce front restartován. Každý správce front musí být definován se systémem sysple-wide, jedinečným 4znakový název subsystému s rozsahem CPF.

Úloha 6: Vytvořit procedury pro správce front IBM MQ

Každý subsystém IBM MQ potřebuje katalogovou proceduru ke spuštění správce front. Můžete vytvořit vlastní nebo použít knihovnu procedur dodané s produktem IBM.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Při migraci z předchozí verze může být nutné upravit katalogizovanou proceduru.*

U každého subsystému IBM MQ definovaného v tabulce názvů subsystémů vytvořte katalogizovanou proceduru v knihovně procedur pro spuštění správce front. Knihovna procedur dodaných IBM se nazývá SYS1.PROCLIB, ale vaše instalace může používat vlastní konvenci pojmenování.

Název procedury spuštěné úlohy správce front je vytvořen zřetěžením názvu subsystému se znaky MSTR. Subsystém CSQ1 má například název procedury CSQ1MSTR. Potřebujete jeden postup pro každý subsystém, který definujete.

Mnoho příkladů a pokynů v této dokumentaci k produktu předpokládá, že máte subsystém CSQ1 . Tyto příklady se mohou snáze používat, pokud je původně vytvořen subsystém CSQ1 pro účely verifikace a testování instalace.

V souboru thlqual.SCSQPROC jsou k dispozici dva ukázkové procedury spuštění ukázky. Člen CSQ4MSTR používá jednu sadu stránek pro každou třídu zprávy, člen CSQ4MSRR používá více sad stránek pro hlavní třídy zprávy. Zkopírujte jednu z těchto procedur do členu xxxxMSTR (kde xxxx je název vašeho

subsystému IBM MQ) vaší SYS1.PROCLIB nebo, pokud nepoužíváte SYS1.PROCLIB, vaše knihovna procedur. Zkopírujte vzorovou proceduru na člena v knihovně procedur pro každý definovaný subsystém IBM MQ .

Když jste členy zkopírovali, můžete je přizpůsobit požadavkům jednotlivých subsystémů, a to za použití pokynů v členu. Informace o určení velikosti oblasti pod hranicí 16 MB, nad hranicí 16 MB a nad čarou 2 GB, najdete v tématu [Doporučené velikosti oblastí](#). Symbolické parametry v souboru JCL můžete také použít k povolení úpravy procedury při jeho spuštění. Máte-li několik subsystémů IBM MQ , můžete zjistit, že je výhodné použít JCL pro společné části postupu, aby se zjednodušila budoucí údržba.

Pokud používáte skupiny sdílení front, musí zřetězení STEPLIB zahrnovat cílovou knihovnu běhového prostředí produktu Db2 SDSNLOAD a musí být autorizována APF. Tato knihovna je vyžadována pouze v zřetězení STEPLIB, pokud není přístupným prostřednictvím seznamu odkazů nebo LPA.

Používáte-li IBM MQ Advanced Message Security zřetězení STEPLIB, musí obsahovat *thlqual.SDRQAUTH* a musí mít autorizaci APF.

Knihovnu uživatelské procedury (CSQXLIB) můžete do této procedury přidat později, chcete-li použít uživatelské procedury správce front. K tomu potřebujete přístup ke knihovně běhového prostředí LE (Language Environment) SCEERUN, pokud se nenachází ve vašem seznamu odkazů (SYS1.PARMLIB(LNKLSTkk)), zřetězte jej v příkazu STEPLIB DD. Je také třeba zastavit a restartovat správce front.

Poznámka: Můžete vytvořit poznámku názvů sady BSDS (bootstrap data set), protokolů a sad stránek pro použití v souboru JCL a poté definovat tyto sady v pozdějším kroku v procesu.

Související pojmy

“Úloha 7: Vytvořit procedury pro inicializátor kanálu” na stránce 539

Pro každý subsystém IBM MQ křejte kopii CSQ4CHIN. V závislosti na tom, jaké další produkty používáte, může být třeba povolit přístup k jiným datovým sadám.

Úloha 7: Vytvořit procedury pro inicializátor kanálu

Pro každý subsystém IBM MQ křejte kopii CSQ4CHIN. V závislosti na tom, jaké další produkty používáte, může být třeba povolit přístup k jiným datovým sadám.

- Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .
- Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.

Je třeba vytvořit proceduru spuštěné úlohy iniciátoru kanálu pro každý subsystém IBM MQ , který bude používat distribuované řazení do fronty.

Postupujte takto:

1. Zkopírujte ukázkovou spuštěnou proceduru úlohy *thlqual.SCSQPROC*(CSQ4CHIN) do knihovny procedur. Pojmenujte proceduru *xxxx CHIN*, kde *xxxx* je název vašeho subsystému IBM MQ (například CSQ1CHIN by byla procedura spuštění úlohy iniciátoru kanálu pro správce front CSQ1).
2. Vytvořte kopii pro každý subsystém IBM MQ , který budete používat.
3. Přizpůsobte postupy dle vašich požadavků podle pokynů v ukázkové proceduře CSQ4CHIN. Symbolické parametry v souboru JCL můžete také použít k povolení úpravy procedury při jeho spuštění. Tento popis je popsán spolu s volbami spuštění v části [Administrace produktu IBM MQ for z/OS](#).

Zřetězete distribuovanou knihovnu front *thlqual.SCSQMVR1*.

Je požadován přístup ke knihovně běhového prostředí LE SCEERUN; pokud není uveden ve vašem seznamu odkazů (SYS1.PARMLIB(LNKLSTkk)), zřetězte jej v příkazu STEPLIB DD.

4. Autorizujte procedury pro spuštění pod vaším externím správcem zabezpečení.

Inicializátor kanálu je dlouhý spuštěný adresový prostor. Chcete-li zabránit jejímu ukončení po spotřebování omezeného množství CPU, potvrďte, že buď:

- Předvolba pro spuštěné úlohy ve vašem systému z/OS je neomezená CPU; konfigurační příkaz JES2 pro JOBCLASS (STC) s TIME = (1440,00) jej dosáhne, nebo
- Explicitně přidejte parametr TIME=1440, nebo TIME=NOLIMIT, do příkazu EXEC pro CSQXJST.

Knihovnu uživatelské procedury (CSQXLIB) můžete do této procedury přidat později, chcete-li použít uživatelské procedury kanálu. Chcete-li to provést, musíte zastavit a restartovat iniciátor kanálu.

Používáte-li zabezpečení SSL, je vyžadována přístupová práva k systémové knihovně SSL (Secure Sockets Layer) systému. Tato knihovna se jmenuje SIEALKE. Knihovna musí mít oprávnění APF.

Pokud používáte protokol TCP/IP, musí být adresní prostor inicializátoru kanálu schopen získat přístup k protokolu TCPIP.DATA datová sada, která obsahuje parametry systému TCP/IP. Způsob, jakým má být datová sada nastavena, závisí na tom, který produkt a rozhraní TCP/IP používáte. Mezi ně patří:

- Proměnná prostředí, RESOLVER_CONFIG
- HFS soubor, /etc/resolv.conf
- // SYSTCPD DD, příkaz
- // SYSTCPDD DD, příkaz
- *jobname/userid.TCPIP.DATA*
- SYS1.TCPPARMS(TCPDATA)
- *zapname.TCPIP.DATA*

Některé z nich mají vliv na kód JCL procedury spuštěné úlohy. Další informace viz [z/OS Communications Server: IP Configuration Guide](#).

Související pojmy

“Úloha 8: Definování subsystému IBM MQ pro třídu služeb z/OS WLM” na stránce 540

Chcete-li v systému z/OS udělit IBM MQ odpovídající prioritu výkonu, musíte přiřadit adresní prostory správce front a inicializátoru kanálu k příslušné třídě služeb správy pracovní zátěže (WLM) produktu z/OS. Pokud to neuděláte explicitně, může se použít nevhodná výchozí nastavení.

Úloha 8: Definování subsystému IBM MQ pro třídu služeb z/OS WLM

Chcete-li v systému z/OS udělit IBM MQ odpovídající prioritu výkonu, musíte přiřadit adresní prostory správce front a inicializátoru kanálu k příslušné třídě služeb správy pracovní zátěže (WLM) produktu z/OS. Pokud to neuděláte explicitně, může se použít nevhodná výchozí nastavení.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ.*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*

Pomocí dialogového okna ISPF dodaného s modulem WLM lze provádět následující úlohy:

- Extrahujte definici zásady správce WLM produktu z/OS z dvojice datových sad WLM.
- Aktualizujte tuto definici zásady přidáním názvů procedur spuštěných úloh iniciátoru správce front a inicializátoru kanálu do vybrané třídy služeb.
- Nainstalujte změněnou zásadu do dvojice datových sad WLM.

Poté aktivujte tuto zásadu pomocí příkazu z/OS.

```
V WLM,POLICY=policyname,REFRESH
```

Další informace o nastavení voleb výkonu najdete v tématu .

Související pojmy

“Úloha 9: Nastavení prostředí Db2” na stránce 541

Používáte-li skupiny sdílení front, musíte vytvořit požadované objekty produktu Db2 přizpůsobením a spuštěním počtu ukázkových úloh.

Úloha 9: Nastavení prostředí Db2

Používáte-li skupiny sdílení front, musíte vytvořit požadované objekty produktu Db2 přizpůsobením a spuštěním počtu ukázkových úloh.

Další informace o výběru prostředí pro ukládání dat, které má být použito, naleznete v části [Rozhodování o úložném prostředí pro odlehčování zátěže](#).

Vyberete-li volbu Db2 jako odlehčování úložného prostředí, postupujte podle části “[Nastavení prostředí produktu Db2](#)” na stránce 541. Pokud vyberete SMDS jako odlehčování úložného prostředí, [prohlédněte si téma Nastavení prostředí SMDS](#). Pokud vybíráte prostředí diskového odlehčování SMDS, budete stále muset nastavit prostředí produktu Db2 pro sdílené fronty.

Nastavení prostředí produktu Db2

Musíte vytvořit a svázat požadované objekty produktu Db2 tím, že upravíte a spustíte několik ukázkových úloh.

- Zopakujte tuto úlohu pro každou skupinu sdílení dat produktu Db2 .
- Možná budete muset provést tuto úlohu při migraci z předchozí verze.
- Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.

Budete-li později chtít použít skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Produkt IBM MQ poskytuje dvě ekvivalentní sady úloh. Ty s předponou CSQ45 jsou z důvodu kompatibility se staršími verzemi produktu IBM MQ a pro použití s produktem Db2 verze 11 a starší. Pokud nastavujete novou skupinu sdílení dat s produktem Db2 V12 nebo novější, doporučujeme používat tyto úlohy s předponou CSQ4X , protože tyto úlohy využívají nejnovější funkce produktu Db2 pro dynamické velikosti a univerzální tabulkové prostory.

Musíte vytvořit prostředí, ve kterém produkt IBM MQ může přistupovat k plánům produktu Db2 a spouštět je v nich používaných pro skupiny sdílení front.

Pro každou novou skupinu sdílení dat produktu Db2 je třeba provést následující kroky. Všechny ukázky JCL se nacházejí v souboru thlqual.SCSQPROC.

1. Upravte a proveďte ukázku JCL CSQ45CSG (nebo CSQ4XCSG) pro vytvoření paměťové skupiny, která má být použita pro databázi IBM MQ , tabulkové prostory a tabulky.
2. Upravte a proveďte ukázku JCL CSQ45CDB (nebo CSQ4XCDB) k vytvoření databáze, kterou mají používat všichni správci front, kteří se připojují k této skupině sdílení dat produktu Db2 .
3. Upravte a proveďte ukázku JCL CSQ45CTS (nebo CSQ4XCTS) a vytvořte tabulkové prostory, které obsahují správce front a tabulky inicializátoru kanálu použité pro skupiny sdílení front (které mají být vytvořeny v kroku 1).
4. Upravte a proveďte ukázku JCL CSQ45CTB (nebo CSQ4XCTB), abyste vytvořili 12 tabulek Db2 a přidružených indexů. Neměňte žádné názvy řádků nebo atributy.
5. Upravte a proveďte ukázku JCL CSQ45BPL (nebo CSQ4XBPL), chcete-li svázat plány produktu Db2 pro správce front, obslužné programy a inicializátor kanálu.
6. Upravte a proveďte ukázku JCL CSQ45GEX (nebo CSQ4XGEX), abyste udělili prováděcí oprávnění k plánům pro ID uživatelů, která jsou použita správcem front, obslužnými programy a inicializačním inicializačním programem kanálu. ID uživatelů pro správce front a inicializátor kanálu jsou uživatelská jména, pod kterými jsou spuštěny procedury spuštěné úlohy. ID uživatele pro obslužné programy jsou ID uživatelů, pod kterými mohou být zadávaná dávková úloha zadána. Názvy příslušných plánů jsou:

Uživatel	Plány
Správce front	CSQ5A 800, CSQ5C 800, CSQ5D 800, CSQ5K 800, CSQ5L 800, CSQ5M 800, CSQ5P 800, CSQ5R 800, CSQ5S 800, CSQ5T 800, CSQ5U 800, CSQ5W 800

Uživatel	Plány
Funkce SDEFS obslužného programu dávky CSQUTIL	CSQ52 800
Obslužné programy CSQ5PQSG a CSQJUCNV	CSQ5B 800
Obslužný program služby CSQUZAP	CSQ5Z 800

V případě selhání během instalace produktu Db2 je možné upravit a provést následující úlohy:

- CSQ45DTB pro zrušení tabulek a indexů.
- CSQ45DTS zruší tabulkové prostory.
- CSQ45DDB pro zrušení databáze.
- CSQ45DSG pro zrušení skupiny úložišť.

Poznámka: Pokud tyto úlohy selžou kvůli problému s uzamčením Db2, je to pravděpodobně způsobeno soupeřením o prostředek Db2, zvláště je-li systém intenzivně využíván. Znovu odešlete úlohy později. Je vhodnější spouštět tyto úlohy, je-li systém lehce použit nebo uveden do klidového stavu.

Další informace o nastavení produktu Db2 naleznete v dokumentu *Db2 10 for z/OS: Db2 Administration*.

Informace o velikostech tabulek Db2 naleznete v příručce [Plánování v systému z/OS](#).

Nastavit prostředí SMDS

SMDS byste měli používat k odlehčování velkých zpráv. Chcete-li poskytnout více kapacity ve vaší struktuře, můžete odlehčovat všechny zprávy do SMDS.

Můžete použít Paměť třídy úložiště (SCM); viz [Použití paměti třídy úložiště se sdílenými frontami](#).

- Odhadněte strukturu a požadavky na prostor datové sady. Viz téma [Pokyny týkající se kapacity sdílené datové sady zpráv](#).
- Přidělit a předformátovat datové sady. Viz téma [Vytvoření datové sady sdílených zpráv](#).
- Chcete-li zobrazit stav **CFLEVEL** a **OFFLOAD**, použijte následující příkaz MQSC.

```
DISPLAY CFSTRUCT(*) CFLEVEL OFFLOAD
```

Další informace o příkazu **DISPLAY CFSTRUCT** naleznete v části [DISPLAY CFSTRUCT](#).

- Pomocí následujících příkazů MQSC se ujistěte, že struktura prostředku Coupling Facility je definována s **CFLEVEL (5)** a **OFFLOAD (SMDS)**:

```
ALTER CFSTRUCT(APP1) CFLEVEL(5)
ALTER CFSTRUCT(APP1) OFFLOAD(SMDS)
```

Další informace o příkazu **ALTER CFSTRUCT** naleznete v tématu [ALTER CFSTRUCT](#).

Související pojmy

[“Úloha 10: Nastavení prostředku Coupling Facility” na stránce 542](#)

Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front ve skupině sdílení front v datové sadě zásad CFRM (coupling facility Resource Management) pomocí adaptéru IXCMIAPU.

Úloha 10: Nastavení prostředku Coupling Facility

Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front ve skupině sdílení front v datové sadě zásad CFRM (coupling facility Resource Management) pomocí adaptéru IXCMIAPU.

- Zopakujte tuto úlohu pro každou skupinu sdílení front.
- Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.
- Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.

Chcete-li později použít skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Všechny struktury pro skupinu sdílení front začínají s názvem skupiny sdílení front. Definujte následující struktury:

- Administrativní struktura s názvem *qsg-name* CSQ_ADMIN. Tato struktura je použita samostatně IBM MQ a neobsahuje žádná uživatelská data.
- Struktura systémové aplikace s názvem *qsg-name* CSQSYSAPPL. Tato struktura je používána systémovými frontami produktu IBM MQ k ukládání informací o stavu.
- Jedna nebo více struktur používaných k zadržení zpráv pro sdílené fronty. Ty mohou mít libovolný název, který vyberete až 16 znaků.
 - První čtyři znaky musí být název skupiny sdílení front. (Je-li název skupiny sdílení front kratší než čtyři znaky, musí být doplněn na čtyři znaky s symboly @.)
 - Pátý znak musí být abecední a následné znaky mohou být abecední nebo numerické. Tato část názvu (bez názvu skupiny sdílení front) je určena pro název CFSTRUCT, když definujete sdílenou frontu nebo objekt struktury CF.

V názvech struktur používaných k ukládání zpráv pro sdílené fronty můžete použít pouze abecední a číselné znaky, nemůžete použít žádné jiné znaky (například znak _, který se používá v názvu administrativní struktury).

Vzorové řídicí příkazy pro IXCMIAPU jsou v datové sadě thlqual.SCSQPROC(CSQ4CFRM). Upravte je a přidejte je do úlohy IXCMIAPU pro prostředek Coupling Facility a spusťte jej.

Když jste úspěšně definovali své struktury, aktivujte zásadu CFRM, která se používá. Chcete-li to provést, zadejte následující příkaz z/OS :

```
SETXCF START,POLICY,TYPE=CFRM,POLNAME= policy-name
```

Informace o strukturách plánování CF a o jejich velikostech naleznete v tématu [Definování prostředků prostředku Coupling Facility](#) .

Související pojmy

“Úloha 11: Implementovat ovládací prvky zabezpečení ESM” na stránce 543

Implementujte obslužné prvky zabezpečení pro skupiny sdílení front, iniciátor kanálu a všechny správce front, kteří mají přístup ke strukturám seznamu prostředku Coupling Facility.

Úloha 11: Implementovat ovládací prvky zabezpečení ESM

Implementujte obslužné prvky zabezpečení pro skupiny sdílení front, iniciátor kanálu a všechny správce front, kteří mají přístup ke strukturám seznamu prostředku Coupling Facility.

- Tuto úlohu opakujte pro každého správce front produktu IBM MQ nebo skupinu sdílení front.
- Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.

Pokud používáte produkt RACF jako externího správce zabezpečení, přečtěte si téma [Nastavení zabezpečení v produktu z/OS](#) , které popisuje, jak implementovat tyto ovládací prvky zabezpečení.

Používáte-li skupiny sdílení front, zkontrolujte, zda jsou ID uživatelů přidružená ke správci front, inicializátoru kanálu a obslužné programy (jak je uvedeno v úloze 9, krok “6” na stránce 541). mít oprávnění k vytvoření připojení RRSF ke každému subsystému Db2 , s nímž chcete navázat spojení. Profil produktu RACF , ke kterému ID uživatele vyžaduje přístup pro čtení, je *DB2ssid.RRSF* ve třídě prostředků DSNR.

Pokud používáte inicializátor kanálu, je třeba provést také následující akce:

- Pokud má váš subsystém aktivní zabezpečení připojení, definujte profil zabezpečení připojení ssid.CHIN do svého externího správce zabezpečení (informace o tomto tématu naleznete v tématu [Profily zabezpečení připojení pro inicializátor kanálu](#)).
- Používáte-li zabezpečení SSL (Secure Sockets Layer) nebo soketové rozhraní, zkontrolujte, zda je ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, konfigurován tak, aby používal produkt UNIX System Services, jak je popsáno v dokumentaci *OS/390 UNIX System Services Planning*.
- Pokud používáte SSL, ujistěte se, že ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je konfigurován pro přístup k souboru svazku klíčů uvedenému v parametru SSLKEYR příkazu ALTER QMGR.

Tito správci front, kteří mají přístup k strukturám seznamu prostředku Coupling Facility, vyžadují odpovídající zabezpečený přístup. Třída RACF je FACILITY. ID uživatele správce front vyžaduje přístup ALTER k serveru IXLSTR. *structure-name* Profil.

Před spuštěním správce front nastavte IBM MQ datovou sadu a zabezpečení systému pomocí:

- Autorizační procedury spuštěné úlohy správce front pro spuštění pod vaším externím správcem zabezpečení.
- Autorizování přístupu k datovým sadám správce front.

Podrobnosti o tom, jak to provést, najdete v tématu [Úlohy instalace zabezpečení pro z/OS\(r\)](#).

Pokud používáte produkt RACF, za předpokladu, že použijete třídu RACF STARTED, není nutné provádět IPL systému (viz [RACF autorizace spuštěných procedur úloh](#)).

Související pojmy

[“Úloha 12: Aktualizace SYS1.PARMLIB členové”](#) na stránce 544

Chcete-li se ujistit, že vaše změny zůstanou v platnosti po IPL, musíte aktualizovat některé členy SYS1.PARMLIB

Úloha 12: Aktualizace SYS1.PARMLIB členové

Chcete-li se ujistit, že vaše změny zůstanou v platnosti po IPL, musíte aktualizovat některé členy SYS1.PARMLIB

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS, na kterém chcete spustit produkt IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že jsou nastavení pro IBM MQ identická na každém systému z/OS v prostředí sysplex.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Aktualizujte SYS1.PARMLIB :

1. Aktualizujte člen IEFSSNss, jak je popsáno v tématu [“Úloha 5: Definujte subsystém IBM MQ na z/OS”](#) na stránce 534.
2. Změňte hodnotu IEASYSpp tak, aby při provádění IPL byly použity následující členy:
 - členy PROGxx nebo IEAAPFaa použité v [“Úloha 2: Autorizace APF pro zaváděcí knihovny produktu IBM MQ”](#) na stránce 532
 - členy LNKLSTkk a LPALSTmm použité v produktu [“Úloha 3: Aktualizace seznamu odkazů z/OS a LPA”](#) na stránce 532
 - Člen SCHEDxx použitý v [“Úloha 4: Aktualizace tabulky vlastností programu z/OS”](#) na stránce 534
 - Člen IEFSSNss používaný v produktu [“Úloha 5: Definujte subsystém IBM MQ na z/OS”](#) na stránce 534

Související pojmy

[“Úloha 13: Úprava vstupních datových sad inicializace”](#) na stránce 545

Vytvořte pracovní kopie vstupních datových sad inicializace a upravte je tak, aby vyhovovala požadavkům vašeho systému.

Úloha 13: Úprava vstupních datových sad inicializace

Vytvořte pracovní kopie vstupních datových sad inicializace a upravte je tak, aby vyhovovala požadavkům vašeho systému.

- Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .
- Při migraci z předchozí verze je třeba provést tuto úlohu.

Každý správce front produktu IBM MQ získává počáteční definice ze série příkazů obsažených v *inicializačních vstupních datových sadách* produktu IBM MQ . Tyto datové sady jsou odkazovány názvy CSQINP1, CSQINP2 a CSQINPT definované v proceduře spuštěné úlohy správce front.

Odezvy na tyto příkazy jsou zapsány do inicializačních výstupních datových sad, na které odkazují názvy CSQOUT1, CSQOUT2 a CSQOUTT (CSQOUT2).

Chcete-li zachovat originály, vytvořte pracovní kopie každého vzorku. Potom můžete upravit příkazy v těchto pracovních kopiích tak, aby odpovídaly požadavkům vašeho systému.

Pokud použijete více než jeden subsystém IBM MQ , pokud zahrnete název subsystému do kvalifikátoru vysoké úrovně názvu vstupní datové sady inicializace, můžete identifikovat subsystém IBM MQ přidružený ke každé datové sadě snadněji.

Další informace o ukázkách naleznete v následujících tématech:

- [Formáty inicializačních datových sad](#)
- [Použití ukázky CSQINP1](#)
- [Použití ukázek CSQINP2](#)
- [Použití ukázky CSQINPX](#)
- [Použití ukázky CSQINPT](#)

Formáty inicializačních datových sad

Vstupní datové sady inicializace mohou být členy rozdělené datové sady (PDS) nebo sekvenční datové sady. Mohou se jednat o zřetězenou řadu datových sad. Definujte je s délkou záznamu 80 bajtů, kde:

- Významné jsou pouze sloupce 1 až 72. Sloupce 73 až 80 se ignorují.
- Záznamy s hvězdičkou (*) ve sloupci 1 jsou interpretovány jako komentáře a jsou ignorovány.
- Prázdné záznamy se ignorují.
- Každý příkaz musí začínat na novém záznamu.
- Koncové-znamená pokračovat od sloupce 1 dalšího záznamu.
- Koncový znak + znamená pokračovat od prvního nemezerových sloupců dalšího záznamu.
- Maximální počet znaků povolených v příkazu je 32 762.

Výstupní datové sady inicializace jsou sekvenční datové sady, s délkou záznamu 125, formátem záznamu VBA a velikostí bloku 629.

Použití ukázky CSQINP1

Datová sada thlqual.SCSQPROC obsahuje dva členy, které obsahují definice fondů vyrovnávacích pamětí, sadu stránek do asociací fondů vyrovnávacích pamětí a příkaz ALTER SECURITY.

Člen CSQ4INP1 používá jednu stránku nastavenou pro každou třídu zprávy. Člen CSQ4INPR používá více sad stránek pro hlavní třídy zprávy.

Začněte odpovídající vzorek do zřetězení CSQINP1 spuštěné procedury úlohy spuštěné správce front.

Notes:

1. IBM MQ podporuje až 16 fondů vyrovnávacích pamětí (nula až 15). Je-li OPMODE nastaven na OPMODE = (NEWFUNC, 800), 100 fondů vyrovnávacích pamětí je podporováno v rozsahu od nuly do 99. Příkaz DEFINE BUFFPOOL může být vydán pouze z inicializační datové sady CSQINP1 . Definice v ukázce uvádějí čtyři fondy vyrovnávacích pamětí.
2. Každá sada stránek použitá správcem front musí být definována v datové sadě inicializace CSQINP1 pomocí příkazu DEFINE PSID. Definice sady stránek přidružuje ID fondu vyrovnávacích pamětí k sadě stránek. Není-li určen žádný fond vyrovnávacích pamětí, je při výchozím nastavení použit nulový fond vyrovnávacích pamětí.

Musí být definována kódová stránka nula (00). Obsahuje všechny definice objektů. Pro každého správce front lze definovat až 100 sad stránek.
3. Příkaz ALTER SECURITY lze použít ke změně atributů zabezpečení TIMEOUT a INTERVAL. V CSQ4INP1 jsou výchozí hodnoty definovány jako 54 pro TIMEOUT a 12 pro INTERVAL.

Informace o uspořádání fondů vyrovnávacích pamětí a sad stránek naleznete v příručce [Plánování v systému z/OS](#) .

Pokud změníte fond vyrovnávacích pamětí a definice sad stránek dynamicky za běhu správce front, měli byste také aktualizovat definice CSQINP1 . Změny se zachovají pouze pro studený start produktu IBM MQ, pokud definice fondu vyrovnávacích pamětí neobsahuje atribut REPLACE.

Použití ukázek CSQINP2

Tato tabulka obsahuje seznam členů thlqual.SCSQPROC , které lze zahrnout do zřetězení CSQINP2 procedury spuštěné úlohy správce front spolu s popisem jejich funkce. Konvence pojmenování je CSQ4INS*. CSQ4INY* bude třeba upravit pro vaši konfiguraci. Měli byste se vyvarovat změny členů CSQINS* , protože budete muset znovu použít jakékoli změny, když migrujete na další vydání. Místo toho můžete vložit příkazy DEFINE nebo ALTER do členů CSQ4INY* .

Tabulka 41. Členové thlqual.SCSQPROC	
Název člena	Popis
CSQ4INSG	Definice systémových objektů.
CSQ4INSA	Systémový objekt a výchozí pravidla pro ověření kanálu.
CSQ4INSX	Definice systémových objektů.
CSQ4INSS	Tento člen můžete upravit a zahrnout, pokud používáte skupiny sdílení front.
CSQ4INSJ	Tento člen upravte a začleňte, pokud používáte publikování/odběr pomocí produktu JMS.
CSQ4INSM	Definice systémových objektů pro zabezpečení rozšířených zpráv.
CSQ4INSR	Upravte a zahrňte tento člen, pokud používáte produkt WebSphere Application Servernebo rozhraní publikování/odběru ve frontě podporované démonem publikování/odběru zařazeného ve frontě v produktu IBM MQ V7 nebo pozdější.
CSQ4DISP	Ukázka CSQINP2 pro zobrazení definic objektů.
CSQ4INYC	Definice klastrování.
CSQ4INYD	Distribuované definice front.
CSQ4INYG	Obecné definice.
CSQ4INYR	Definice tříd úložišť, použití více sad stránek pro hlavní třídy zprávy.
CSQ4INYS	Definice tříd úložišť pomocí jedné sady stránek pro každou třídu zprávy.

Musíte definovat objekty pouze jednou, ne vždy, když spustíte správce front, takže není nutné tyto definice zahrnout do CSQINP2 pokaždé. Pokud je zahrnete pokaždé, pokoušíte se definovat objekty, které již existují, a budete mít podobné zprávy jako následující:

```
CSQM095I +CSQ1 CSQMAQLC QLOCAL(SYSTEM.DEFAULT.LOCAL.QUEUE) ALREADY EXISTS
CSQM090E +CSQ1 CSQMAQLC FAILURE REASON CODE X'00D44003'
CSQ9023E +CSQ1 CSQMAQLC ' DEFINE QLOCAL ' ABNORMAL COMPLETION
```

Tyto objekty nejsou poškozeny tímto selháním. Chcete-li ponechat datovou sadu definic SYSTEM v zřetězení CSQINP2 , můžete se vyhnout zprávám o selhání tím, že uvedete atribut REPLACE pro každý objekt.

Použití vzorku CSQINPX

Ukázka `thlqual.SCSQPROC(CSQ4INPX)` obsahuje sadu příkazů, které byste mohli chtít provést při každém spuštění inicializátoru kanálu. Jedná se obvykle o příkazy související s kanály, jako je například START LISTENER, které se požadují při každém spuštění inicializátoru kanálu, nikoli vždy při spuštění správce front a které nejsou povoleny ve vstupních datových sadách CSQINP1 nebo CSQINP2. Tuto ukázku si musíte před použitím upravit; můžete ji pak zahrnout do datové sady CSQINPX pro iniciátor kanálu.

Příkazy IBM MQ obsažené v datové sadě jsou prováděny na konci inicializace inicializátoru kanálu a výstup se zapisuje do datové sady určené příkazem CSQOUTX DD. Výstup je podobný výstupu, který je vytvořen funkcí COMMAND obslužného programu IBM MQ (CSQUTIL). Další podrobnosti najdete v tématu [Obslužný program CSQUTIL](#) .

Můžete zadat kterýkoli z příkazů IBM MQ , které lze vydat z CSQUTIL, nikoli pouze příkazy kanálu. Můžete zadávat příkazy z jiných zdrojů, zatímco je CSQINPX zpracováván. Všechny příkazy jsou vydávány v pořadí bez ohledu na úspěch předchozího příkazu.

Chcete-li určit dobu odezvy příkazu, můžete použít příkaz pseudo-command jako první příkaz v datové sadě. To trvá jedno volitelné klíčové slovo RESPTIME (*nnn*), kde *nnn* je doba čekání na odpověď na každý příkaz, v sekundách. To je v rozsahu od 5 do 999; předvolba je 30.

Pokud IBM MQ zjistí, že odpovědi na čtyři příkazy zabraly příliš dlouho, zpracování CSQINPX je zastaveno a žádné další příkazy nejsou vydány. Inicializátor kanálu není zastaven, ale zpráva [CSQU052E](#) je zapsána do datové sady CSQOUTX a zpráva [CSQU013E](#) je odeslána na konzolu.

Když produkt IBM MQ úspěšně dokončil zpracování objektu CSQINPX, odešle se na konzolu zpráva [CSQU012I](#) .

Použití ukázky CSQINPT

Tato tabulka obsahuje seznam členů `thlqual.SCSQPROC` , které lze zahrnout do zřetězení CSQINPT u procedury spuštěné úlohy správce front, s popisem jejich funkce.

Tabulka 42. Členové <code>thlqual.SCSQPROC</code>	
Název člena	Popis
CSQ4INST	Výchozí definice odběru systému.
CSQ4INYT	Definice publikování/odběru.

Příkazy IBM MQ obsažené v datové sadě jsou provedeny při dokončení inicializace publikování/odběru a výstup je zapisován do datové sady určené příkazem CSQOUTT DD. Výstup je podobný výstupu, který je vytvořen funkcí COMMAND obslužného programu IBM MQ (CSQUTIL). Další podrobnosti najdete v tématu [Obslužný program CSQUTIL](#) .

Související pojmy

[“Úloha 14: Vytvoření zaváděcího programu a datových sad protokolu” na stránce 548](#)

Pomocí dodaného programu CSQJU003 připravte zaváděcí datové sady (BSDSs) a datové sady protokolů.

Úloha 14: Vytvoření zaváděcího programu a datových sad protokolu

Pomocí dodaného programu CSQJU003 připravte zaváděcí datové sady (BSDSs) a datové sady protokolů.

- Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .
- Při migraci z předchozí verze není třeba provést tuto úlohu.

Ukázkové řídicí příkazy jazyka JCL a služby Access Method (AMS) ke spuštění CSQJU003 pro vytvoření jednoho nebo duálního prostředí protokolování se budou konat v souboru thlqual.SCSQPROC(CSQ4BSDS). Upravte a spusťte tuto úlohu, abyste vytvořili BSDS a protokoly a předformátujete protokoly.

Důležité: Měli byste použít nejnovější verzi souboru CSQ4BSDS nebo aktualizovat JCL ručně pro použití RECORDS (850 60).

Procedura spuštěné úlohy, CSQ4MSTR, popsána v tématu [“Úloha 6: Vytvořit procedury pro správce front IBM MQ”](#) na stránce 538, odkazuje na BSDSs v příkazech ve tvaru:

```
//BSDS1 DD DSN=++HLQ++.BSDS01,DISP=SHR
//BSDS2 DD DSN=++HLQ++.BSDS02,DISP=SHR
```

Na datové sady protokolu odkazuje BSDSs.

Poznámka:

1. Příkaz BLKSIZE musí být zadán v příkazu SYSPRINT DD v kroku LOGDEF. Hodnota BLKSIZE musí být 629.
2. Chcete-li usnadnit identifikaci sad dat pro samozavedení a datových sad protokolů z různých správců front, začleňte název subsystému do kvalifikátoru vyšší úrovně těchto datových sad.
3. Používáte-li skupiny sdílení front, musíte definovat zaváděcí program a protokolové datové sady s hodnotou SHAREOPTIONS (2 3).

Chcete-li získat informace o plánování zaváděcího programu a datových sad protokolů a jejich velikosti, prohlédněte si příručku [Plánování v systému z/OS](#) .

Pro produkt IBM MQ 8.0 zlepšuje rozšíření protokolu RBA protokolu o velikosti 8 bajtů dostupnost správce front, jak je popsáno v tématu [Větší relative Byte Address Byte](#). Chcete-li před prvním spuštěním správce front povolit osmibajtovou adresu RBA protokolu, proveďte po vytvoření svého prostředí protokolování následující kroky.

1. Pomocí **IDCAMS ALTER** přejmenujte formát BSDSs formátu verze 1 (vytvořený pomocí programu CSQJU003) k něčemu jako ++HLQ++.V1.BSDS01.

Poznámka: Ujistěte se, že jste přejmenovali komponenty dat a indexu stejně jako klastr VSAM.

2. Přidělte nové BSDS se stejnými atributy jako ty, které již byly definovány. Tato hodnota se stane formátem BSDSs formátu verze 2, který bude použit správcem front při jeho spuštění.
3. Spusťte obslužný program převodu BSDS (CSQJUCNV) pro převod sady BSD verze 1 na novou verzi BSDSs formátu 2.
4. Jakmile je konverze úspěšně dokončena, odstraňte BSDSs formátu verze 1.
5. Chcete-li použít 8bajtový protokol RBA, ujistěte se, že Verze 8.0 nové funkce jsou povoleny s OPMODE, jak je popsáno v [“Úloha 17: Přizpůsobte modul parametrů systému”](#) na stránce 550.

Poznámka: Je-li správce front ve skupině sdílení front, musí být všichni správci front ve skupině sdílení front spuštěni s operačním systémem OPMODE (NEWFUNC,800) předtím, než lze povolit protokol 8bajtového protokolu adresy RBA.

Související pojmy

[“Úloha 15: Definujte sady stránek”](#) na stránce 549

Nadefinujte sady stránek pro každého správce front pomocí jednoho z dodaných ukázek.

Úloha 15: Definujte sady stránek

Nadefinujte sady stránek pro každého správce front pomocí jednoho z dodaných ukázek.

- Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .
- Při migraci z předchozí verze není třeba provést tuto úlohu.

Definujte oddělené sady stránek pro každého správce front IBM MQ . thlqual.SCSQPROC(CSQ4PAGE) a thlqual.SCSQPROC(CSQ4PAGR) obsahují řídicí příkazy JCL a AMS k definování a formátování sad stránek. Člen CSQ4PAGE používá jednu sadu stránek pro každou třídu zprávy, člen CSQ4PAGR používá více sad stránek pro hlavní třídy zprávy. JCL spouští dodaný obslužný program CSQUTIL. Přezkoumejte ukázky a upravte je podle počtu sad stránek, které chcete, a velikosti, které se mají použít. Informace o sadách stránek a o tom, jak vypočítat vhodné velikosti, naleznete v příručce Plánování v systému z/OS .

Procedura spuštění úlohy CSQ4MSTR popsaná v “Úloha 6: Vytvořit procedury pro správce front IBM MQ” na stránce 538 odkazuje na sady stránek, v příkazu ve tvaru:

```
//CSQP00 nn DD DISP=OLD,DSN= xxxxxxxxx
```

kde *nn* je číslo sady stránek mezi 00 a 99 a *xxxxxxxxxx* je datová sada, kterou definujete.

Poznámka:

1. Hodláte-li používat funkci rozšíření dynamické sady stránek, ujistěte se, že jsou pro každou sadu stránek definovány sekundární fyzické oblasti. thlqual.SCSQPROC(CSQ4PAGE) ukazuje, jak to provést.
2. Chcete-li pomoci identifikovat sady stránek z různých správců front, zahrňte název subsystému do kvalifikátoru vyšší úrovně datové sady přidružené ke každé sadě stránek.
3. Pokud chcete povolit volbu FORCE, která má být použita spolu s funkcí FORMAT obslužného programu CSQUTIL, musíte přidat atribut REUSE na příkaz AMS DEFINE CLUSTER. Tento popis je popsán v publikaci Administrace produktu IBM MQ for z/OS.
4. Pokud mají být vaše sady stránek větší než 4 GB, musíte použít funkci EXTENDED ADDRESABILITY systému SMS (Storage Management System).

Související pojmy

“Úloha 16: Přidání položek IBM MQ do tabulek Db2” na stránce 549

Používáte-li skupiny sdílení front, spusťte obslužný program CSQ5PQSG pro přidání skupin sdílení front a položek správce front do tabulek produktu IBM MQ ve skupině sdílení dat produktu Db2 .

Úloha 16: Přidání položek IBM MQ do tabulek Db2

Používáte-li skupiny sdílení front, spusťte obslužný program CSQ5PQSG pro přidání skupin sdílení front a položek správce front do tabulek produktu IBM MQ ve skupině sdílení dat produktu Db2 .

- Zopakujte tuto úlohu pro každou skupinu sdílení front produktu IBM MQ a každého správce front.
- Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.
- Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.

Chcete-li později použít skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Pro každou skupinu sdílení front a pro každého správce front, který má být členem skupiny sdílení front, spusťte program CSQ5PQSG . (CSQ5PQSG je popsáno v publikaci Administrace produktu IBM MQ for z/OS.)

Proveďte následující akce v uvedeném pořadí:

1. Přidejte položku skupiny sdílení front do tabulek produktu IBM MQ Db2 pomocí funkce ADD QSG programu CSQ5PQSG . Ukázku lze poskytnout v souboru thlqual.SCSQPROC(CSQ45AQS).

Provedte tuto funkci jednou pro každou skupinu sdílení front, která je definována ve skupině sdílení dat produktu Db2 . Položka skupiny sdílení front musí existovat před přidáním jakýchkoli položek správce front, které odkazují na skupinu sdílení front.

2. Přidejte položku správce front do tabulek produktu IBM MQ verze Db2 pomocí funkce ADD QMGR programu CSQ5PQSG . Ukázku lze poskytnout v souboru thlqual.SCSQPROC(CSQ45AQM).

Tuto funkci provedte pro každého správce front, který má být členem skupiny sdílení front.

Poznámka:

- a. Správce front může být členem pouze jedné skupiny sdílení front.
- b. Chcete-li používat skupiny sdílení front, musí být spuštěna služba RRS.

Související pojmy

“Úloha 17: Přizpůsobte modul parametrů systému” na stránce 550

Modul parametrů systému IBM MQ řídí prostředí protokolování, archivace, trasování a připojení, které IBM MQ používá při své operaci. Je dodáván výchozí modul, nebo můžete vytvořit vlastní pomocí dodaných zdrojových modulů JCL a assembleru.

Úloha 17: Přizpůsobte modul parametrů systému

Modul parametrů systému IBM MQ řídí prostředí protokolování, archivace, trasování a připojení, které IBM MQ používá při své operaci. Je dodáván výchozí modul, nebo můžete vytvořit vlastní pomocí dodaných zdrojových modulů JCL a assembleru.

- *Podle potřeby opakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Při migraci z předchozí verze je třeba provést tuto úlohu. Podrobné informace naleznete v tématu [Migrace a upgrade produktu IBM MQ](#).*
- *Chcete-li povolit produkt IBM MQ Advanced Message Security for z/OS v existujícím správci front, stačí nastavit parametr SPLCAP na hodnotu YES, jak je popsáno v tématu “[Použití CSQ6SYSP](#)” na stránce 552. Pokud konfiguruje tohoto správce front poprvé, dokončete celou tuto úlohu.*

Modul parametrů systému má tři následující makra:

Název makra	Účel
CSQ6SYSP	Určuje parametry připojení a trasování, viz “ Použití CSQ6SYSP ” na stránce 552 .
CSQ6LOGP	Ovládá inicializaci protokolu, viz “ Použití CSQ6LOGP ” na stránce 561
CSQ6ARVP	Řídí inicializaci archivu, viz “ Použití CSQ6ARVP ” na stránce 565

Produkt IBM MQ dodává výchozí modul parametrů systému CSQZPARM, který je vyvolán automaticky, pokud zadáte příkaz START QMGR (bez parametru PARM) ke spuštění instance produktu IBM MQ. CSQZPARM je v knihovně autorizace APF thlqual.SCSQAUTH také dodána s IBM MQ. Hodnoty těchto parametrů se zobrazí jako série zpráv, když spustíte IBM MQ.

Další informace o použití tohoto příkazu najdete v části [START QMGR](#) .

Vytvoření vlastního modulu parametrů systému

Pokud CSQZPARM neobsahuje požadované systémové parametry, můžete vytvořit svůj vlastní modul parametrů systému pomocí vzorového souboru JCL uvedeného v souboru thlqual.SCSQPROC(CSQ4ZPRM).

Chcete-li vytvořit vlastní modul parametrů systému, postupujte takto:

1. Vytvořte pracovní kopii ukázky JCL.
2. Upravte parametry pro každé makro v kopii podle potřeby. Pokud odeberete všechny parametry z volání makra, výchozí hodnoty se automaticky vyzvednou za běhu.

3. Nahradte zástupný symbol ++NAME++ názvem, který má načíst zaváděcí modul (tento může být CSQZPARM).
4. Pokud váš assembler není assembler vysoké úrovně, změňte kód JCL podle požadavků vašeho assembleru.
5. Spuštěním skriptu JCL sestavte a propojte úpravy upravených verzí maker systémových parametrů tak, aby vytvářeli modul načítání. Jedná se o nový modul parametrů systému s názvem, který jste zadali.
6. Vložte zaváděcí modul vytvořený v uživatelské knihovně s oprávněním APF.
7. Přidejte uživatelský přístup pro čtení k uživatelské knihovně oprávněných uživatelů APF.
8. Zahrňte tuto knihovnu do procedury úlohy STEPLIB pro spuštěnou úlohu správce front produktu IBM MQ . Tento název knihovny musí být uveden před knihovnou thlqual.SCSQAUTH v knihovně STEPLIB.
9. Při spuštění správce front vyvolejte nový modul parametrů systému. Je-li například nový modul pojmenován NEWMODS, zadejte následující příkaz:

```
START QMGR PARM(NEWMODS)
```

10. Ujistěte se o úspěšném dokončení příkazu kontrolou protokolu úlohy. Záznam by měl být v protokolu podobný následujícímu:

```
CSQ9022I CDL1 CSQYASCP 'START QMGR' NORMAL COMPLETION
```

Můžete také zadat název modulu parametrů ve spouštěcím skriptu JCL správce front. Další informace naleznete v tématu [Spuštění a zastavení správce front](#).

Poznámka: Pokud si zvolíte pojmenování svého modulu CSQZPARM, nemusíte uvádět parametr PARM v příkazu START QMGR.

Podrobné vyladění modulu parametrů systému

Produkt IBM MQ také dodává sadu tří zdrojových modulů assembleru, které lze použít k dokončení vyladění existujícího modulu parametrů systému. Tyto moduly jsou v knihovně thlqual.SCSQASMS. Tyto moduly zpravidla použijete v testovacím prostředí ke změně výchozích parametrů v makrech parametrů systému. Každý zdrojový modul volá jiné makro parametru systému:

Tento zdrojový modul assembler ...	Vyvolá toto makro ...
CSQFSYSP	CSQ6SYSP (parametry připojení a trasování)
CSQJLOGP	CSQ6LOGP (inicializace protokolu)
CSQJARVP	CSQ6ARVP (inicializace archivu)

Tímto způsobem můžete používat tyto moduly:

1. Vytvoření pracovních kopií každého modulu zdroje v assembleru v knihovně assembleru uživatele.
2. Upravte své kopie přidáním nebo změnou hodnot jakýchkoli parametrů podle potřeby.
3. Sestavte své kopie všech upravených modulů a vytvořte moduly objektů v knihovně uživatelských objektů.
4. Odkaz na úpravy těchto modulů kódu objektu s existujícím modulem parametrů systému za účelem vytvoření modulu zavedení, který je novým modulem parametrů systému.
5. Ujistěte se, že nový modul systémových parametrů je členem autorizované knihovny uživatele.
6. Zahrňte tuto knihovnu do procedury úlohy STEPLIB spuštěné úlohy správce front. Tato knihovna musí být uvedena před knihovnou thlqual.SCSQAUTH v knihovně STEPLIB.

7. Vyvolejte nový modul parametrů systému zadáním příkazu START QMGR, zadáním nového názvu modulu v parametru PARM, jako dříve.

Ukázkový usermod je poskytován ve členu CSQ4UZPR SCSQPROC, který demonstruje, jak spravovat upravené systémové parametry pod kontrolou SMP/E.

Změna systémových parametrů

Při spuštění správce front můžete změnit některé systémové parametry. Informace o příkazech [SET SYSTEM](#), [SET LOGa](#) [SET ARCHIVE](#) naleznete v následujících příkazech.

Vložení příkazů SET do vstupních datových sad inicializace tak, aby nabyly účinnosti při každém spuštění správce front.

Související pojmy

“Úloha 18: Přizpůsobte parametry inicializátoru kanálu” na stránce 572

Pomocí příkazu ALTER QMGR můžete upravit inicializátor kanálu tak, aby vyhovoval vašim požadavkům.

Použití CSQ6SYSP

Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6SYSP.

Výchozí parametry pro CSQ6SYSPa to, zda můžete změnit jednotlivé parametry pomocí příkazu SET SYSTEM, jsou zobrazeny v Tabulka 43 na stránce 552. Chcete-li některou z těchto hodnot změnit, přečtěte si podrobné popisy parametrů.

Tabulka 43. Výchozí hodnoty parametrů CSQ6SYSP			
Parametr	Popis	Výchozí hodnota	příkaz SET
ACELIM	Velikost fondu úložišť ACE v blocích o velikosti 1 KB.	0 (bez omezení)	✓
CCACHE	Určuje typ mezipaměti klastru, který má být použit.	STATICKÝ	-
CMDUSER	Výchozí ID uživatele pro kontroly zabezpečení příkazů.	CSQOPR	-
CONNSWAP	Určuje, zda úlohy, které vydávají určité volání rozhraní API produktu IBM MQ , jsou typu swaponovatelný nebo negapovatelný.	YES	-
EXCLMSG	Uvádí seznam zpráv, které mají být vyloučeny z jakéhokoli protokolu. Zprávy v tomto seznamu se neodešlou do konzoly z/OS a do protokolu hardcopy. Výsledkem použití parametru EXCLMSG k vyloučení zpráv je efektivnější z perspektivy CPU než použití metod popsaných v “Úloha 22: Potlačit informační zprávy” na stránce 576	()	✓
EXITLIM	Doba (v sekundách), po kterou mohou být uživatelské procedury správce front spuštěny během každého vyvolání.	30	-
EXITTCB	Počet spuštěných úloh serveru, které mají být použity ke spuštění správce front.	8	-
LOGLOAD	Počet záznamů protokolu zapsaných pomocí IBM MQ mezi začátkem jednoho kontrolního bodu a dalším.	500 000	✓

Tabulka 43. Výchozí hodnoty parametrů CSQ6SYSP (pokračování)

Parametr	Popis	Výchozí hodnota	příkaz SET
MULCCAPT	Určuje vlastnost Naměřená cena využití, která řídí algoritmus pro shromažďování dat používaných měřenými licenčními poplatky za použití (MULC).	Viz popis parametru	-
RežimOp	Řídí režim činnosti správce front.	Viz popis parametru	-
OMMAKON	Parametry připojení OTMA.	Viz popis parametru	-
QINDXBLD	Určuje, zda bude restartování správce front čekat, než budou všechny indexy znovu sestaveny nebo budou dokončena před přestavením všech indexů.	WAIT	-
QMCCSID	Identifikátor kódované znakové sady pro správce front.	Nula	-
QSGDATA	Parametry skupiny sdílení front.	Viz popis parametru	-
RESAUDIT	parametr monitorování RESLEVEL.	YES	-
ROUTCDE	Směrovací kód zprávy přiřazený zprávám, které nejsou vyžádané z určité konzoly.	1	-
SERVICE	Rezervováno pro použití produktem IBM.	0	✓
SMFACCT	Určuje, zda mají být shromažďována data evidence SMF při spuštění správce front. Všimněte si, že data evidence kanálu třídy 4 jsou shromažďována pouze v případě, že je spuštěn inicializátor kanálu.	NO	-
SMFSTAT	Určuje, zda má být shromažďována statistika SMF při spuštění správce front. Všimněte si, že statistická data o inicializátoru kanálu třídy 4 jsou shromažďována pouze v případě, že je spuštěn inicializátor kanálu.	NO	-
SPLCAP	Určuje, zda je v tomto správci front povolena funkce zásad zabezpečení fronty. Pro IBM MQ Advanced Message Security for z/OS nastavte tento parametr na YES.	NO	-
STATIME	Výchozí čas, v minutách, mezi každým shromážděním statistických údajů.	30	✓
TRACSTR	Určuje, zda má být trasování spuštěno automaticky.	NO	-
TRACTBL	Velikost trasovací tabulky v blocích o velikosti 4 KB, která má být použita prostředkem globálního trasování.	99 (396 KB)	✓
WLMTIME	Doba mezi skenováním indexu fronty pro fronty spravované WLM.	30	-
WLMTIMU	Jednotky (minuty nebo sekundy) pro operaci WLMTIME.	minuty	-

ACELIM

Určuje maximální velikost fondu úložišť ACE v 1kB blocích. Číslo musí být v rozsahu 0-999999. Výchozí hodnota nula znamená, že nejsou určena žádná omezení nad rámec možností systému.

Hodnotu ACELIM byste měli nastavit pouze pro správce front, u nichž bylo zjištěno nadměrné používání úložiště ECSA. Omezení fondu úložišť ACE je limitováno počtem připojení v systému, a tedy množstvím úložiště ECSA používané správcem front.

Jakmile správce front dosáhne limitu, není možné pro aplikace získat nová připojení. Nedostatek nových připojení způsobí selhání ve zpracování MQCONN a u aplikací koordinovaných prostřednictvím služby RRS bude pravděpodobně docházet k selháním v nějakém rozhraní IBM MQ API.

Položka řízení přístupu (ACE) představuje přibližně 12,5 % z celkové hodnoty ECSA vyžadované pro řídicí bloky připojení, které souvisí s podprocesy. Takže například při zadání parametru ACELIM=5120 by se očekávalo omezení celkového množství ECSA přidělených správcem front (pro řídicí bloky související s podprocesy) přibližně na 40960K; , což je 5120 krát 8.

Pro omezení částky celkové částky ECSA přidělené správcem front pro řídicí bloky související s podprocesy na 5120K je požadována hodnota ACELIM 640.

Prostřednictvím záznamů SMF 115 subtype 7 zhotovovaných trasováním statistiky CLASS(3) lze monitorovat velikost fondu úložišť 'ACE/PEB, a následně nastavit vhodnou hodnotu ACELIM.

Informaci, jaké celkové množství úložiště ECSA používá správce front pro řídicí bloky, lze získat ze záznamů SMF 115 subtype 7 zapisovaných trasováním statistiky CLASS(2); jsou to první dva společně přidávané prvky v QSRSPHBT.

Poznámka: Nastavení ACELIM by mělo sloužit jako mechanismus k ochraně obrazu z/OS před špatným chováním správce front, nikoli jako prostředek k řízení připojení aplikací ke správci front.

CCACHE

Určuje typ mezipaměti klastru, který má být použit. Další informace viz [“Konfigurace klastru správce front”](#) na stránce 216.

STATICKÝ

Je-li mezipaměť klastru statická, její velikost je pevně daná při spuštění správce front, což je dostatečné pro aktuální množství informací o klastru a navíc i prostor pro rozšíření. Velikost nelze zvýšit, je-li správce front aktivní. Toto nastavení je výchozí.

DYNAMICKÝ

Je-li mezipaměť klastru dynamická, počáteční velikost alokovaná při spuštění správce front může být automaticky zvýšena, je-li to nutné, zatímco je správce front aktivní.

CMDUSER

Uvádí výchozí ID uživatele použité pro kontroly zabezpečení příkazu. Toto ID uživatele musí být definováno pro ESM (například RACF). Zadejte název o délce 1 až 8 alfanumerických znaků. První znak musí být písmeno.

Předvolba je CSQOPR.

CONNSWAP

Určuje, zda jsou dávkové úlohy, které vydávají určité volání rozhraní API produktu IBM MQ, za dobu trvání požadavku rozhraní API produktu IBM MQ přebušovatelne nebo negappitelné. Uvedte jednu z následujících hodnot:

NO

Úlohy jsou během určitých volání rozhraní API produktu IBM MQ neswapovat.

YES

Úlohy jsou ve všech voláních rozhraní API produktu IBM MQ přelíhnutelné.

Výchozí hodnota je Ano.

Tento parametr použijte, pokud jsou úlohy s nízkou prioritou odloženy tak, že jsou zadrženy prostředky IBM MQ, na které by mohly čekat jiné úlohy nebo úlohy. Tento parametr nahrazuje parametr služby, který byl zahrnut IBM MQ V701; , který parametr služby již není používán.

IBM MQ zobrazení WebSphere Application Server jako součást prostředí RRSBATCH. Při použití klíčového slova CONNSWAP z produktu IBM WebSphere MQ 7.1 se použije na všechny aplikace v prostředí BATCH nebo RRSBATCH. Klíčové slovo CONNSWAP lze použít také pro uživatele TSO, nelze jej však použít pro aplikace CICS nebo IMS. Změny CONNSWAP se provedou, když se provede recyklace správce front. Recykl je vyžadován po provedení změny klíčového slova, protože makro CSQ6SYSP je znovu sestaveno a správce front je restartován pomocí modulu načítání, který je aktualizován makrem.

Alternativně lze adresní prostor WebSphere Application Server nastavit jako negapovatelný pomocí PPT.

EXCLMSG

Uvádí seznam chybových zpráv, které mají být vyloučeny.

Tento seznam je dynamický a je aktualizován pomocí příkazu SET SYSTEM.

Výchozí hodnota je prázdný seznam ().

Zprávy se dodávají bez předpony CSQ a bez přípony kódu akce (I-D-E-A). Chcete-li například vyloučit zprávu CSQX500I, přidejte X500 do tohoto seznamu. Tento seznam může obsahovat maximálně 16 identifikátorů zpráv.

Aby mohla být tato zpráva zařazena do seznamu, musí být vydána po normálním spuštění v adresních prostorech MSTR nebo CHIN a začínat jedním z následujících znaků E, H, I, J, L, M, N, P, R, T, V, W, X, Y, 2, 3, 5, 9.

Identifikátory zpráv, které jsou vydány jako výsledek zpracování příkazů, mohou být přidány do seznamu, avšak nebudou vyloučeny. Například, identifikátor zprávy je vydán jako výsledek příkazu DISPLAY USAGE PSID (*), tato zpráva však nemůže být potlačena.

EXITLIM

Určuje dobu (v sekundách) povolenou pro každé vyvolání správce front. (Tento parametr nemá žádný vliv na uživatelské procedury kanálu.)

Uveďte hodnotu v rozsahu 5 až 9999.

Výchozí hodnota je 30. Správce front vyzývá procedury, které jsou spuštěny každých 30 sekund. U každého typu poll jsou všechny, které byly spuštěny déle, než je čas určený produktem EXITLIM, vynuceně ukončeny.

EXITTCB

Určuje počet spuštěných úloh serveru, které mají být použity ke spuštění uživatelských procedur ve správci front. (Tento parametr nemá žádný vliv na uživatelské procedury kanálu.) Musíte zadat číslo alespoň tak vysoké, jako je maximální počet uživatelských procedur (jiných než uživatelských procedur kanálu), které může správce front spustit, jinak dojde k selhání s abend 6c6.

Uveďte hodnotu v rozsahu 0 až 99. Hodnota nula znamená, že žádné uživatelské procedury nelze spustit.

Výchozí hodnota je 8.

LOGLOAD

Určuje počet záznamů protokolu, které produkt IBM MQ zapisuje mezi začátkem jednoho kontrolního bodu a dalším. Produkt IBM MQ zahájí nový kontrolní bod po zapsání počtu záznamů, které zadáte.

Zadejte hodnotu v rozsahu 200 až 16 000 000.

Výchozí hodnota je 500 000.

Čím vyšší je hodnota, tím lepší je výkon produktu IBM MQ; Nicméně restartování trvá déle, je-li parametr nastaven na velkou hodnotu.

Doporučené nastavení:

Testovací systém 10 000

Produkční systém 500 000

V produkčním systému může dodaná výchozí hodnota vést k příliš vysoké frekvenci kontrolních bodů.

Hodnota volby LOGLOAD určuje frekvenci kontrolních bodů správce front. Příliš velká hodnota znamená, že velké množství dat je zapsáno do protokolu mezi kontrolními body, což vede k vyššímu času restartování zotavení správce front, který následuje po selhání. Příliš nízká hodnota způsobuje, že se kontrolní body vyskytují příliš často při špičkovém zatížení, nepříznivě ovlivňují doby odezvy a využití procesoru.

Pro LOGLOAD je doporučována počáteční hodnota 500 000. Pro četnost trvalých zpráv o velikosti 1 kB 100 zpráv za sekundu (tj. 100 MQPUT s potvrzením a 100 MQGET s potvrzováním) je interval mezi kontrolními body přibližně 5 minut.

Poznámka: To je určeno pouze jako vodítko a optimální hodnota pro tento parametr je závislá na charakteristikách jednotlivých systémů.

MULCCAPT

Určuje algoritmus, který má být použit pro shromažďování dat používaných měřenými licenčními poplatky za použití (MULC).

STANDARD

MULTC je založen na čase volání MQCONN rozhraní API produktu IBM MQ na dobu volání MQDISC rozhraní API produktu IBM MQ .

Upřesněno

MULTC je založen na čase od začátku volání API IBM MQ na konec volání API IBM MQ .

Výchozí hodnota je STANDARD.

OPMODE=(Režim, ÚroveňVerifikace)

OPMODE uvádí provozní režim správce front.

Výchozí nastavení parametru OPMODE je OPMODE=(COMPAT , 800) .

Režim

Uvádí požadovaný provozní režim. Hodnoty jsou následující:

COMPAT

Správce front se bude provozovat v režimu kompatibility. Některé nové funkce nebudou dostupné. Správce front lze migrovat zpět na starší verzi.

NEWFUNC

Všechny nové funkce poskytované na této úrovni kódu jsou k dispozici. Správce front nelze migrovat zpět na starší verzi.

VerificationLevel

VerificationLevel je kód Version.Release.Modification (VRM) bez interpunkce; 800například.

Hodnota parametru *ÚroveňVerifikace* zajišťuje, aby se parametry **CSQ6SYSP** kódovaly pro použití s úrovní kompilovaného makra **CSQ6SYSP**. Pokud se *ÚroveňVerifikace* neshoduje s úrovní VRM, kterou používá SCSQMACS pro **CSQ6SYSP**, bude nahlášena chyba kompilace. *ÚroveňVerifikace* se kompiluje do modulu parametru.

Pokud se při spuštění správce front neshoduje *ÚroveňVerifikace* s úrovní verze správce front, vynutí se použití režimu COMPAT.

Účelem parametru *ÚroveňVerifikace* je vyhnout se neúmyslnému a nevratnému nastavení parametru OPMODE na NEWFUNC. K této chybě může dojít při migraci na novější verzi produktu IBM MQ pomocí příkazů **CSQ6SYSP** připravených pro starší verzi správce front. Dojít k ní může i v případě, že používáte modul parametru **CSQ6SYSP** vystavěný se starší verzí maker SCSQMACS.

OMMAKON

Parametry OTMA. Toto klíčové slovo má pět pozičních parametrů::

OTMACON = (Group , Member , Druexit , Age , Tpipepfx)

Skupina

Jedná se o název skupiny XCF, do které patří tato konkrétní instance produktu IBM MQ .

Může být 1 až 8 znaků dlouhý a musí být zadán velkými písmeny.

Výchozí hodnota je prázdná, což znamená, že produkt IBM MQ se nesmí pokoušet o připojení ke skupině XCF.

Člen

Jedná se o název člena této konkrétní instance produktu IBM MQ ve skupině XCF.

Může být 1 až 16 znaků dlouhý a musí být zadán velkými písmeny.

Předvolba je 4znakový název správce front.

Druexit

Uvádí název uživatelské procedury rozpoznání cíle OTMA, která má být spuštěna produktem IMS.

Může mít délku 1 až 8 znaků.

Předvolba je DFSYDRUO.

Tento parametr je volitelný; je povinný, pokud má IBM MQ přijímat zprávy z aplikace IMS , která nebyla spuštěna produktem IBM MQ. Název musí odpovídat uživatelské proceduře rozpoznání místa určení, která je kódována v systému IMS . Další informace viz [“Použití uživatelských procedur OTMA v produktu IMS”](#) na stránce 630.

Věk

Představuje dobu, v sekundách, po kterou je ID uživatele z produktu IBM MQ považováno za dříve ověřené IMS.

Může být v rozsahu nula až 2 147 483 647.

Výchozí hodnota je 2 147 483 647.

Doporučuje se nastavit tento parametr ve spojení s parametrem `interval` příkazu ALTER SECURITY tak, aby byla zachována konzistence nastavení mezipaměti zabezpečení v rámci sálového počítače.

Tpipepfx

To představuje předponu, která se má použít pro názvy Tpipe.

Skládá se ze tří znaků; první znak je v rozsahu A až Z, následné znaky jsou A až Z nebo 0 až 9. Výchozí hodnota je CSQ.

Toto se použije pokaždé, když produkt IBM MQ vytvoří Tpipe; zbytek názvu je přiřazen pomocí IBM MQ. Nelze nastavit úplný název Tpipe pro všechny nástroje Tpipe vytvořené produktem IBM MQ.

QINDXBLD

Určuje, zda bude restartování správce front čekat, dokud nebudou všechny indexy fronty znovu sestaveny nebo budou pokračovat, než budou znovu sestaveny všechny indexy.

WAIT

Restartování správce front čeká na dokončení všech sestavení indexu fronty. To znamená, že během normálního zpracování rozhraní API produktu IBM MQ během vytváření indexu nejsou zpožděny žádné aplikace, protože všechny indexy jsou vytvořeny dříve, než se mohou k tomuto správci front připojit všechny aplikace.

Toto nastavení je výchozí.

NoWait

Správce front lze restartovat, než bude dokončena veškerá sestavení indexu fronty.

QMCCSID

Určuje výchozí identifikátor kódované znakové sady, který má správce front (a tedy i distribuované fronty) používat.

Uvedte hodnotu v rozsahu nula až 65535. Hodnota musí představovat kódovou stránku EBCDIC uvedenou jako nativní kódovou stránku z/OS pro zvolený jazyk v [národních jazycích](#).

Nula, což je předvolená hodnota, znamená použít CCSID momentálně nastavený, nebo, pokud žádný není nastaven, použijte CCSID 500. To znamená, že pokud jste explicitně nastavili hodnotu CCSID na jakoukoli jinou než nulovou hodnotu, nemůžete ji resetovat nastavením hodnoty QMCCSID na nulu; nyní musíte použít správný nenulový CCSID. Je-li QMCCSID nula, můžete zkontrolovat, jaké CCSID se skutečně používá, vydáním příkazu DISPLAY QMGR CCSID.

Na distribuovaných platformách použijte příkaz [ALTER QMGR](#) .

QSGDATA

Data skupiny sdílení front. Toto klíčové slovo má pět pozičních parametrů:

QSGDATA = (Qsgname , Dsgname , Db2name , Db2serv , Db2blob)

QSGNAME

Jedná se o název skupiny sdílení front, do níž patří správce front.

Platné znaky naleznete v tématu [Pravidla pojmenování objektů IBM MQ](#) . Název:

- Může mít délku 1 až 4 znaky.
- Nesmí začínat číslicí
- Nesmí končit znakem @.

Důvodem je to, že z důvodů implementace jsou názvy méně než čtyř znaků doplněny interně znaky @ symbolům,

Výchozí hodnotou je prázdné místo, které označuje, že správce front není členem žádné skupiny sdílení front.

Dsgname

Jedná se o název skupiny sdílení dat produktu Db2 , ke které se má správce front připojit.

Může být 1 až 8 znaků dlouhý a musí být zadán velkými písmeny.

Výchozí hodnotou je prázdná místa, která označuje, že nepoužíváte skupiny sdílení front.

Db2name

Jedná se o název subsystému Db2 nebo připojení skupiny, ke kterému se má správce front připojit.

Může být 1 až 4 znaky dlouhé a musí být zadáno velkými písmeny.

Výchozí hodnotou je prázdná místa, která označuje, že nepoužíváte skupiny sdílení front.

Poznámka: Subsystém Db2 (nebo příloha skupiny) musí být ve skupině sdílení dat Db2 zadané v produktu Dsgnamea všichni správci front musí určovat stejnou skupinu sdílení dat produktu Db2 .

Db2serv

Jedná se o počet úloh serveru použitých pro přístup k produktu Db2.

Může být v rozsahu od 4 do 10.

Výchozí hodnota je 4.

Db2blob

Jedná se o počet úloh produktu Db2 použitých pro přístup k binárním objektům BLOB (Binary Large Objects).

Může být v rozsahu od 4 do 10.

Výchozí hodnota je 4.

Uvedete-li jeden z parametrů názvu (tj. **Qsgname**, **Dsgname** nebo **Db2name**), musíte zadat hodnoty pro ostatní názvy, jinak IBM MQ selže.

RESAUDIT

Uvádí, zda jsou záznamy auditu RACF zapsány pro kontroly zabezpečení RESLEVEL prováděné během zpracování připojení.

Zadejte jednu z následujících možností:

NO

Monitorování RESLEVEL se neprovádí.

YES

Auditování RESLEVEL se provádí.

Výchozí hodnota je ANO.

ROUTCODE

Určuje výchozí směrovací kód zprávy produktu z/OS přiřazený zprávám, které nejsou odesílány v přímé odpovědi na příkaz MQSC.

Zadejte jednu z následujících možností:

1. Hodnota v rozsahu od 1 do 16 včetně.
2. Seznam hodnot oddělených čárkou a uzavřený v závorkách. Každá hodnota musí být v rozsahu od 1 do 16 včetně.

Výchozí hodnota je 1.

Další informace o kódech směrování příkazu z/OS naleznete v příručce *MVS Routing and Descriptor Codes*.

SERVICE

Toto pole je vyhrazeno pro použití produktem IBM.

SMFACCT

Určuje, zda produkt IBM MQ odesílá data evidence do prostředí SMF automaticky při spuštění správce front.

Zadejte jednu z následujících možností:

NO

Nezahajujte automatické shromažďování účetních dat.

YES

Spustit shromažďování dat evidence automaticky pro výchozí třídu 1.

celá čísla

Seznam tříd, pro které se evidence shromažďuje automaticky v rozsahu 1 až 4.

Výchozí hodnota je NO.

SMFSTAT

Určuje, zda mají být shromažďovány statistické údaje SMF automaticky při spuštění správce front.

Zadejte jednu z následujících možností:

NO

Nezahajujte automaticky shromažďování statistických údajů.

YES

Automaticky zahájit shromažďování statistiky pro výchozí třídu 1.

celá čísla

Seznam tříd, pro které se statistiky shromažďují automaticky v rozsahu od 1 do 4.

Výchozí hodnota je NO.

SPLCAP

Schopnost zásad zabezpečení umožňuje vyšší úroveň zabezpečení zpráv prostřednictvím zásad, které řídí, zda jsou zprávy podepisovány nebo šifrovány, jak jsou napsány a čteny z front.

Jeho použití je licencováno samostatně instalovaným produktem IBM MQ Advanced Message Security (AMS), který dodává modul povolení v knihovně SDRQAUTH.

Zpracování zásad zabezpečení je pro tohoto správce front povoleno konfigurací funkce SPLCAP s některou z následujících hodnot:

NO

Možnost implementace zásad zabezpečení zpráv pro fronty není povolena během inicializace správce front.

YES

Schopnosti zabezpečení zpráv jsou povoleny během inicializace správce front.

Je-li tento ovládací prvek nastaven, správce front se během inicializace pokusí načíst modul povolující licenci ze souboru SDRQAUTH a spustit další adresní prostor (AMSM).

Správce front se nespustí, pokud je licence AMS licencována a že je v místě nutná konfigurace zabezpečení zpráv.

Výchozí hodnota je NO.

STATIME

Určuje výchozí dobu (v minutách) mezi po sobě jdoucími shromažďováními statistických údajů.

Uveďte číslo v rozsahu 0 až 1440.

Pokud zadáte hodnotu nula, jsou statistická data i data evidence shromažďována v plošné zprávě shromažďování dat SMF. Informace o nastavení této funkce najdete v tématu [Použití nástroje pro správu systému](#).

Výchozí hodnota je 30.

TRACSTR

Uvádí, zda se má globální trasování spustit automaticky.

Zadejte jednu z následujících možností:

NO

Nespouštět globální trasování automaticky.

YES

Spustí globální trasování automaticky pro výchozí třídu, třídu 1.

celá čísla

Seznam tříd, pro které má být globální trasování spuštěno automaticky v rozsahu od 1 do 4.

Automaticky spustit globální trasování pro všechny třídy.

Výchozí hodnota je NO, pokud v makru nezadáte klíčové slovo.

Poznámka: Dodaný výchozí zaváděcí modul parametru systému (CSQZPARM) má TRACTSTR=YES (nastaveno v modulu assembleru CSQFSYSP). Pokud nechcete automaticky spustit trasování, buď vytvořte svůj vlastní modul parametrů systému, nebo vydejte příkaz STOP TRACE poté, co byl spuštěn správce front.

Podrobné informace o příkazu STOP TRACE naleznete v části [STOP TRACE](#).

TRACTBL

Určuje výchozí velikost v blocích o velikosti 4 kB v tabulce trasování, kde prostředek globálního trasování ukládá trasovací záznamy IBM MQ.

Uveďte hodnotu v rozsahu od 1 do 999.

Výchozí hodnota je 99. To je ekvivalentní 396 KB.

Poznámka: Paměť pro trasovací tabulku je alokována v ECSA. Proto je třeba tuto hodnotu vybrat s opatrností.

WLMTIME

Určuje dobu (v minutách nebo sekundách, v závislosti na hodnotě WLMTIMU) mezi jednotlivými skenováními indexů ve frontách spravovaných pomocí WLM.

Uveďte hodnotu v rozsahu od 1 do 9999.

Výchozí hodnota je 30.

WLMTIMU

Časové jednotky použité s parametrem WLMTIME.

Zadejte jednu z následujících možností:

minuty

WLMTIME představuje počet minut.

s

WLMTIME představuje počet sekund.

Výchozí hodnota je MINS.

Související odkazy

[“Použití CSQ6LOGP” na stránce 561](#)

Toto téma použijte jako referenci, jak určit volby protokolování pomocí CSQ6LOGP.

[“Použití CSQ6ARVP” na stránce 565](#)

Toto téma slouží jako reference, jak určit své archivační prostředí pomocí CSQ6ARVP

Použití CSQ6LOGP

Toto téma použijte jako referenci, jak určit volby protokolování pomocí CSQ6LOGP.

Použijte CSQ6LOGP k vytvoření voleb protokolování.

Výchozí parametry pro CSQ6LOGPa to, zda můžete změnit každý parametr pomocí příkazu [SET LOG](#) , jsou zobrazeny v [Výchozí hodnoty parametrů CSQ6LOGP](#). Potřebujete-li změnit některou z těchto hodnot, přečtěte si podrobné popisy parametrů.

Parametr	Popis	Výchozí hodnota	příkaz SET
COMPLOG	Řídí, zda je komprese protokolu povolena.	ŽÁDNÉ	X
DEALLCT	Doba, kdy archivní pásková jednotka zůstává nevyužita, než bude dealokována.	zero	X
INBUFF	Velikost úložiště vstupní vyrovnávací paměti pro aktivní a archivní datové sady žurnálu.	60 KB	-
MAXARCH	Maximální počet svazků protokolu archivace, které lze zaznamenat.	500	X
MAXCNOFF	Maximální počet úloh odlehčování CSQJOFF7 , které lze spustit paralelně.	31	-
MAXRTU	Maximální počet vyhrazených páskových jednotek alokovaných pro souběžné čtení páskových nosičů s protokolem archivace.	2	X
OFFLOAD	Archivování zapnuto nebo vypnuto.	ANO (ZAPNUTO)	-

Tabulka 44. Výchozí hodnoty parametrů CSQ6LOGP (pokračování)

Parametr	Popis	Výchozí hodnota	příkaz SET
<u>OUTBUFF</u>	Velikost úložiště výstupní vyrovnávací paměti pro aktivní a archivní datové sady žurnálu.	4 000 KB	-
<u>TWOACTV</u>	Jedno nebo duální aktivní protokolování.	ANO (duální)	-
<u>TWOARCH</u>	Jednoduché nebo duální protokolování archivace.	ANO (duální)	-
<u>TWOBSDS</u>	Jeden nebo dva BS DS.	ANO (duální BS DS)	-
<u>WRTHRSH</u>	Počet výstupních vyrovnávacích pamětí, které mají být vyplněny, než jsou zapsány do aktivních protokolových datových sad.	20	X

COMPLOG

Uvádí, zda je komprese protokolu povolena.

Uveďte buď:

ŽÁDNÉ

Komprese protokolu není povolena.

RLE

Komprese protokolu je povolena za použití kódování run-length.

ANY

Správce front vybere kompresní algoritmus, který poskytuje největší stupeň komprese záznamu protokolu. Tato volba má za následek kompresi RLE.

Výchozí hodnota je NONE.

Další informace o kompresi protokolu viz [Komprese protokolu](#).

DEALLCT

Uvádí dobu v minutách, po kterou může pásková jednotka pro čtení archivu zůstat nevyužita, než bude dealokována.

Uveďte jednu z následujících možností:

- Čas, v minutách, v rozsahu 0 až 1440
- NOLIMIT

Uvedením 1440 nebo NOLIMIT znamená, že pásková jednotka není nikdy dealokována.

Výchozí hodnota je nula.

Při čtení dat protokolu archivace z pásky se doporučuje nastavit tuto hodnotu dostatečně vysokou, aby umožňovala IBM MQ optimalizovat obsluhu pásek pro více aplikací čtení.

INBUFF

Uvádí velikost vstupní vyrovnávací paměti (v kilobajtech) pro čtení aktivních a archivních protokolů během obnovy. Použijte dekadické číslo v rozsahu 28 až 60. Uvedená hodnota je zaokrouhlena nahoru na násobek 4.

Výchozí hodnota je 60 kB.

Doporučené nastavení:

Testovací systém 28 KB

Produkční systém 60 KB

Nastavte ji na maximum pro nejlepší výkon při čtení protokolu.

MAXARCH

Uvádí maximální počet svazků protokolu archivace, které lze zaznamenat v BSDS. Po překročení tohoto počtu začne záznam znovu na začátku BSDS.

Použijte dekadické číslo v rozsahu od 10 do 1000.

Výchozí hodnota je 500.

Doporučené nastavení:

Testovací systém 500 (výchozí)

Produkční systém 1 000

Nastavte toto na maximum tak, aby BSDS mohlo zaznamenávat tolik protokolů, kolik je možné.

Informace o protokolech a BSDS naleznete v tématu [Správa prostředků produktu IBM MQ](#).

MAXCNOFF

Určuje počet úloh odlehčování CSQJOFF7 , které lze spustit paralelně.

To umožňuje vyladit správce front nebo správce front tak, že nebudou používat všechny dostupné páskové jednotky.

Místo toho správce front před pokusem o přidělení nových datových sad archivu vyčká, dokud nebude dokončena úloha odsunutí CSQJOFF7 .

Pokud správce front provádí archivaci na pásku, nastavte tento parametr tak, aby počet souběžných požadavků na pásku neměl být roven nebo větší než počet dostupných páskových jednotek, v opačném případě by systém mohl reagovat.

Mějte na paměti, že pokud se používá duální archivace, pak každá úloha odkládání provádí oba archivy, takže je třeba tento parametr nastavit odpovídajícím způsobem. Je-li například správce front dual archivovat na pásku, hodnota MAXCNOFF=2 umožní archivaci dvou aktivních protokolů souběžně se čtyřmi páskami.

Pokud několik správců front sdílí páskové jednotky, měli byste nastavit hodnotu MAXCNOFF pro každého správce front odpovídajícím způsobem.

Výchozí hodnota je 31.

Uveďte hodnotu v rozsahu od 1 do 31.

MAXRTU

Uvádí maximální počet vyhrazených páskových jednotek, které mohou být alokovány souběžně pro čtení páskových nosičů s protokolem archivace.

Tento parametr a parametr DEALLCT umožňují produktu IBM MQ optimalizovat čtení protokolu archivu z páskových zařízení.

Uveďte hodnotu v rozsahu od 1 do 99.

Výchozí nastavení je 2.

Doporučuje se, abyste nastavili hodnotu tak, aby byla alespoň o jeden menší než počet páskových jednotek, které jsou k dispozici pro produkt IBM MQ. Jinak byste mohli odložit proces odlehčování, což by mohlo ovlivnit výkon vašeho systému. Pro maximální propustnost při zpracování protokolu archivace určete největší možnou hodnotu této volby a nezapomeňte, že pro zpracování odkládání je třeba použít alespoň jednu páskovou jednotku.

OFFLOAD

Určuje, zda je archivace zapnuta nebo vypnuta.

Uveďte buď:

YES

Archivace je zapnuta

NO

Archivace je vypnutá

Výchozí hodnota je ANO.

Upozornění: Pokud pracujete v testovacím prostředí, vypněte archivaci produktu **ne**, pokud nepracujete. Pokud jej vypnete, nemůžete zaručit, že data budou obnovena v případě selhání systému nebo transakce.

OUTBUFF

Uvádí celkovou velikost úložiště, které má být použito IBM MQ pro výstupní vyrovnávací paměti pro zápis aktivních a archivních souborů dat protokolu, v kilobajtech. Každá výstupní vyrovnávací paměť má velikost 4 kB.

Parametr musí být v rozsahu od 80 do 4000. Uvedená hodnota je zaokrouhlena nahoru na násobek 4. Hodnoty mezi 40 a 80 budou akceptovány z důvodu kompatibility a jsou považovány za hodnotu 80.

Výchozí hodnota je 4 000 kB.

Doporučené nastavení:

Testovací systém 400 KB

Produkční systém 4 000 KB

Nastavte tuto hodnotu na maximum, abyste se vyhnuli překročení vyrovnávací paměti výstupu protokolu.

TWOACTV

Uvádí jednoduché nebo duální aktivní protokolování.

Uveďte buď:

NO

Jednotlivý aktivní protokol

YES

Duální aktivní protokoly

Výchozí hodnota je ANO.

Další informace o použití jednoho a duálního protokolování naleznete v tématu [Správa prostředků produktu IBM MQ](#).

TWOARCH

Určuje počet protokolů archivu, které produkt IBM MQ produkuje, když je aktivní protokol odložen.

Uveďte buď:

NO

Jednoduché archivní protokoly

YES

Duální archivní protokoly

Výchozí hodnota je ANO.

Doporučené nastavení:

Testovací systém NO

Produkční systém ANO (výchozí)

Další informace o použití jednoho a duálního protokolování naleznete v tématu [Správa prostředků produktu IBM MQ](#).

TWOBSDS

Určuje počet zaváděcích datových sad.

Uveďte buď:

NO

Jediný BSDS

YES

Duální BSDS

Výchozí hodnota je ANO.

Další informace o použití jednoho a duálního protokolování naleznete v tématu [Správa prostředků produktu IBM MQ](#).

WRTHRS

Uvádí počet výstupních vyrovnávacích pamětí o velikosti 4 kB, které mají být vyplněny, než jsou zapsány do aktivních datových sad protokolu.

Čím větší je počet vyrovnávacích pamětí, tím méně často dochází k zápisu, a tím se zlepší výkon produktu IBM MQ. Vyrovnávací paměti mohou být zapsány před tímto číslem, pokud se vyskytnou významné události, jako např. bod potvrzení.

Uveďte počet vyrovnávacích pamětí v rozsahu od 1 do 256.

Výchozí hodnota je 20.

Související odkazy

[“Použití CSQ6SYSP” na stránce 552](#)

Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6SYSP.

[“Použití CSQ6ARVP” na stránce 565](#)

Toto téma slouží jako reference, jak určit své archivační prostředí pomocí CSQ6ARVP

Použití CSQ6ARVP

Toto téma slouží jako reference, jak určit své archivační prostředí pomocí CSQ6ARVP

Použijte CSQ6ARVP k vytvoření vašeho prostředí archivace.

Výchozí parametry pro CSQ6ARVPa to, zda můžete změnit každý parametr pomocí příkazu SET ARCHIVE, jsou zobrazeny v [Tabulka 45 na stránce 565](#).

Pokud je pravděpodobné, že volné místo na archivním svazku DASD bude fragmentováno, doporučuje se uvést menší primární oblast a povolit rozšíření do sekundárních fyzických oblastí. Další informace o přidělení prostoru pro aktivní protokoly najdete v tématu [Plánování archivního úložiště protokolu](#).

Parametr	Popis	Výchozí hodnota	příkaz SET
ALCUNIT	Jednotky, ve kterých jsou provedena alokace primárního a sekundárního prostoru.	BLK (bloky)	X
ARCPFX1	Předpona pro název první datové sady archivního protokolu.	CSQARC1	X
ARCPFX2	Předpona pro název druhé datové sady archivního protokolu.	CSQARC2	X
ARCRETN	Doba uchování datové sady protokolu archivace ve dnech.	9999	X
ARCWRTC	Seznam kódů přenosové cesty pro zprávy operátorovi o datových sadách protokolu archivu.	1,3,4	X
ARCWTOR	Zda se má odeslat zpráva operátorovi a čekat na odpověď před pokusem o připojení datové sady protokolu archivu.	YES	X

Tabulka 45. Výchozí hodnoty parametrů CSQ6ARVP (pokračování)

Parametr	Popis	Výchozí hodnota	příkaz SET
BLKSIZE	Velikost bloku datové sady protokolu archivu.	28 672	X
CATALOG	Zda jsou archivní datové sady protokolu katalogizovány v ICF.	NO	X
COMPACT	Zda mají být datové sady protokolu archivace kompaktní.	NO	X
PRIQTY	Primární přidělení prostoru pro datové sady DASD.	25 715	X
PROTECT	Zda jsou datové sady protokolu archivace chráněny profily ESM při vytváření datových sad.	NO	X
QUIESCE	Maximální čas (v sekundách) povolený pro uvedení do klidového stavu při uvedení ARCHIVE LOG s uvedeným MODE (QUIESCE).	5	X
SECQTY	Sekundární přidělení prostoru pro datové sady DASD. Prohlédněte si parametr ALCUNIT pro jednotky, které se mají použít.	540	X
TSTAMP	Určuje, zda má název archivní datové sady obsahovat časové razítko.	NO	X
UNIT	Typ zařízení nebo název jednotky, na které je uložena první kopie datových sad protokolu archivace.	Páska	X
UNIT2	Typ zařízení nebo název jednotky, na které je uložena druhá kopie datových sad protokolu archivace.	Prázdný	X

ALCUNIT

Uvádí jednotku, ve které jsou prováděny alokace primárního a sekundárního prostoru.

Zadejte jednu z následujících možností:

CYL

Válce

TRK

Stopy

BLK

Bloky

Doporučuje se použít BLK, protože je nezávislý na typu zařízení.

Výchozí hodnota je BLK.

Pokud je pravděpodobné, že volné místo na archivním svazku DASD bude fragmentováno, doporučuje se uvést menší primární oblast a povolit rozšíření do sekundárních fyzických oblastí. Další informace o přidělení prostoru pro aktivní protokoly naleznete v příručce [Plánování v systému z/OS](#).

ARCPFX1

Uvádí předponu pro název první datové sady archivního protokolu.

Popis způsobu pojmenování datových sad a omezení délky ARCPFX1 najdete v parametru TSTAMP.

Tento parametr nemůže zůstat prázdný.

Výchozí hodnota je CSQARC1.

Je možné, že budete muset autorizovat ID uživatele přidružené k adresnímu prostoru správce front produktu IBM MQ a vytvořit archivní protokoly s touto předponou.

ARCPFX2

Uvádí předponu pro název druhé datové sady archivního protokolu.

Viz parametr TSTAMP pro popis způsobu pojmenování datových sad a omezení délky ARCPFX2.

Tento parametr nemůže být prázdný ani v případě, že parametr TWOMARCH je zadán jako NO.

Výchozí hodnota je CSQARC2.

Je možné, že budete muset autorizovat ID uživatele přidružené k adresnímu prostoru správce front produktu IBM MQ a vytvořit archivní protokoly s touto předponou.

ARCRETN

Uvádí období uchování, ve dnech, které má být použito při vytvoření datové sady protokolu archivace.

Parametr musí být v rozsahu nula až 9999.

Výchozí hodnota je 9999.

Doporučené nastavení:

Testovací systém

3

V testovacím systému se archivní protokoly pravděpodobně nepožadují po dlouhou dobu.

Produkční systém

9 999 (výchozí)

Chcete-li efektivně vypnout automatické odstranění protokolu archivace, nastavte tuto hodnotu vysokou hodnotu.

Další informace o zrušení datových sad protokolu archivace naleznete v tématu [Vyřazování datových sad protokolu archivace](#).

ARCWRTC

Uvádí seznam směrovacích kódů z/OS pro zprávy o datových sadách protokolu archivace na operátora. Toto pole je ignorováno, pokud je parametr ARCWTOR nastaven na hodnotu NO.

Uveďte až 14 směrovacích kódů, každý s hodnotou v rozsahu od 1 do 16. Je třeba určit alespoň jeden kód. Oddělte kódy v seznamu čárkami, nikoli mezerami.

Předvolba je seznam hodnot: 1,3,4.

Další informace o kódech směrování příkazu z/OS naleznete v příručce *MVS Routing and Descriptor Codes*.

ARCWTOR

Určuje, zda má být odeslána zpráva operátorovi a přijata odezva před pokusem o připojení datové sady protokolu archivace.

Ostatní uživatelé produktu IBM MQ by mohli být nuceni počkat, než bude datová sada připojena, pokud však produkt IBM MQ čeká na odezvu na zprávu, nemá to na ně vliv.

Uveďte buď:

YES

Zařízení potřebuje dlouhou dobu k připojení datových sad protokolu archivu. Například pásková jednotka.

NO

Zařízení nemá dlouhé prodlevy. Například DASD.

Výchozí hodnota je ANO.

Doporučené nastavení:

Testovací systém	NO
Produkční systém	ANO (výchozí) To je závislé na provozních postupech. Pokud se používají páskové roboty, NO může být vhodnější.

BLKSIZE

Určuje velikost bloku datové sady protokolu archivu. Velikost bloku, kterou uvedete, musí být kompatibilní s typem zařízení, které jste uvedli v parametru UNIT.

Parametr musí být v rozsahu 4 097 až 28 672. Hodnota, kterou zadáte, je zaokrouhlena na násobek hodnoty 4 096.

Předvolba je 28 672.

Tento parametr je přepsaný velikostí bloku třídy dat subsystému správy úložiště (SMS), pokud je zadán.

Je-li datová sada protokolu archivace zapsána do DASD, doporučuje se zvolit maximální velikost bloku, který umožňuje 2 bloky pro každou stopu. Pro zařízení 3390 byste například měli použít velikost bloku 24 576.

Je-li datová sada protokolu archivace zapsána na pásku, určení největší možné velikosti bloku zlepšuje rychlost čtení protokolu archivace. Měli byste použít velikost bloku 28 672.

Doporučené nastavení:

Testovací systém	Doporučení velikosti bloku použijte v závislosti na médiích použitých pro protokoly archivace. To je, pro disk 24 576, a páska 28 672.
Produkční systém	Doporučení velikosti bloku použijte v závislosti na médiích použitých pro protokoly archivace. To je, pro disk 24 576, a páska 28 672.

CATALOG

Uvádí, zda jsou datové sady protokolu archivace katalogovány v primárním katalogu ICF (integrated catalog facility).

Uveďte buď:

NO

Archivní datové sady protokolu nejsou katalogizovány.

YES

Archivní datové sady protokolů jsou katalogizovány.

Výchozí hodnota je NO.

Všechny datové sady protokolu archivace přidělené v DASD musí být katalogizovány. Pokud archivujete do DASD s parametrem CATALOG nastaveným na NO, zobrazí se zpráva CSQJ072E pokaždé, když je přidělena datová sada protokolu archivace, a IBM MQ katalogizuje datovou sadu.

Doporučené nastavení:

Testovací systém	YES
Produkční systém	ANO, jsou-li archivy alokovány na DASD

COMPACT

Uvádí, zda data zapisovaná do protokolů archivu mají být optimalizována. Tato možnost se používá u zařízení 3480 nebo 3490 s funkcí IDRC (Improved Data Recording Capability). Pokud je tato funkce zapnuta, zapisuje hardware v páskové řídicí jednotce data s daleko vyšší hustotou, než je obvyklé, což

umožňuje na každém nosiči uložit více dat. Uvedte NO, pokud nepoužíváte zařízení 3480 s funkcí IDRC nebo základní model 3490, kromě 3490E. Uvedte ANO, pokud chcete, aby data byla zhuštěna.

Uvedte buď:

NO

Neoptimalizovat datové sady

YES

Optimalizovat datové sady

Výchozí hodnota je NO.

Zadání YES nepříznivě ovlivní výkon. Také si uvědomte, že data komprimovaná na pásku lze číst pouze pomocí zařízení, které podporuje funkci IDRC. To může být problém, pokud budete muset odeslat archivní pásky do jiného serveru pro vzdálenou obnovu.

Doporučené nastavení:

Testovací systém Nelze použít

Produkční systém NE (výchozí)

Toto platí pouze pro kompresi IDR 3480 a 3490. Nastavení této hodnoty na YES může při obnově degradovat výkon při čtení a restartování protokolu archivace. Neovlivní to zápis na pásku.

PRIQTY

Určuje přidělení primárního prostoru pro datové sady DASD v systému ALCUNITs.

Hodnota musí být větší než nula.

Výchozí hodnota je 25 715.

Tato hodnota musí být dostatečná pro kopii datové sady protokolu nebo odpovídající BSDS, podle toho, která z těchto hodnot je větší. Chcete-li určit potřebnou hodnotu, proveďte následující kroky:

1. Určete počet přidělených aktivních záznamů protokolu (c), jak je vysvětleno v tématu [“Úloha 14: Vytvoření zaváděcího programu a datových sad protokolu”](#) na stránce 548.
2. Určete počet 4096 bajtových bloků v každém bloku protokolu archivu:

$$d = \text{BLKSIZE} / 4096$$

kde BLKSIZE je zaokrouhlená hodnota.

3. Pokud ALCUNIT = BLK:

$$\text{PRIQTY} = \text{INT}(c / d) + 1$$

kde INT znamená zaokrouhlit dolů na celé číslo.

Pokud ALCUNIT = TRK:

$$\text{PRIQTY} = \text{INT}(c / (d * \text{INT}(e/\text{BLKSIZE}))) + 1$$

kde e je počet bajtů pro každou stopu (56664 pro zařízení 3390) a INT znamená zaokrouhlit dolů na celé číslo.

Pokud ALCUNIT = CYL:

$$PRIQTY = INT(c / (d * INT(e/BLKSIZE) * f)) + 1$$

kde f je počet stop pro každou cylindru (15 pro zařízení 3390) a INT znamená zaokrouhlit dolů na celé číslo.

Informace o tom, jak velké, aby váš protokol a archivní datové sady zpřístupníte, viz “Úloha 14: Vytvoření zaváděcího programu a datových sad protokolu” na stránce 548 a “Úloha 15: Definujte sady stránek” na stránce 549.

Doporučené nastavení:

Testovací systém 1 680

Dostatečný k zadržení celého aktivního protokolu, to znamená:

$$10 \ 080 / 6 = 1 \ 680 \text{ blocks}$$

Produkční systém Nelze použít při archivaci na pásku.

Pokud je pravděpodobné, že volné místo na archivním svazku DASD bude fragmentováno, doporučuje se uvést menší primární oblast a povolit rozšíření do sekundárních fyzických oblastí. Další informace o přidělení prostoru pro aktivní protokoly naleznete v příručce [Plánování v systému z/OS](#).

PROTECT

Uvádí, zda mají být datové sady protokolu archivace chráněny diskretními profily ESM (externího správce zabezpečení) při vytváření datových sad.

Uveďte buď:

NO

Profily nejsou vytvářeny.

YES

Diskretní profily datové sady jsou vytvářeny při odlehčování protokolů. Uvedete-li ANO:

- Ochrana ESM musí být aktivní pro IBM MQ.
- ID uživatele přidružené k adresnímu prostoru správce front produktu IBM MQ musí mít oprávnění k vytváření těchto profilů.
- Pokud archivujete na pásku, musí být třída TAPEVOL aktivní.

V opačném případě dojde k selhání odlehčování.

Výchozí hodnota je NO.

QUIESCE

Uvádí maximální dobu v sekundách povolenou pro uvedení do klidového stavu, je-li zadán příkaz ARCHIVE LOG s uvedeným MODE (QUIESCE).

Parametr musí být v rozsahu od 1 do 999.

Výchozí nastavení je 5.

SECQTY

Určuje alokaci sekundárního prostoru pro datové sady DASD v systému ALCUNITs. Sekundární oblast může být alokována až 15krát; podrobnosti naleznete v příručce *z/OS MVS JCL Reference* a *z/OS MVS JCL User's Guide*.

Parametr musí být větší než nula.

Výchozí hodnota je 540.

TSTAMP

Uvádí, zda název datové sady protokolu archivace obsahuje časovou značku.

Uved'te buď:

NO

Názvy nezahrnujte časovou značku. Datové sady protokolu archivace jsou pojmenovány:

```
arcpxi.A nnnnnn
```

Kde *arcpxi* je předpona názvu datové sady zadaná pomocí ARCPFX1 nebo ARCPFX2. *arcpxi* může mít až 35 znaků.

YES

Názvy obsahují časové razítko. Datové sady protokolu archivace jsou pojmenovány:

```
arcpxi.cyyddd.T hhmsst.A nnnnnn
```

kde c je 'D' pro roky až do roku 1999 nebo 'E' pro rok 2000 a novější a *arcpxi* je předpona názvu datové sady zadaná pomocí ARCPFX1 nebo ARCPFX2. *arcpxi* může mít až 19 znaků.

EXT

Názvy obsahují časové razítko. Datové sady protokolu archivace jsou pojmenovány:

```
arcpxi.D yyyddd.T hhmsst.A nnnnnn
```

Kde *arcpxi* je předpona názvu datové sady zadaná pomocí ARCPFX1 nebo ARCPFX2. *arcpxi* může mít až 17 znaků.

Výchozí hodnota je NO.

UNIT

Uvádí typ zařízení nebo název jednotky zařízení, které se používá k uložení první kopie datové sady archivního protokolu.

Uved'te typ zařízení nebo název jednotky 1 až 8 alfanumerických znaků. První znak musí být písmeno.

Tento parametr nemůže být prázdný.

Předvolba je TAPE.

Pokud archivujete do DASD, můžete uvést generický typ zařízení s omezeným rozsahem svazku, například UNIT=3390.

Pokud archivujete do DASD, ujistěte se, že:

- Přidělení primárního prostoru je dostatečně velké, aby obsahovalo všechna data z aktivních datových sad protokolů.
- Volba katalogu datových sad protokolu archivace (CATALOG) je nastavena na hodnotu YES.
- Použili jste vhodnou hodnotu parametru BLKSIZE.

Pokud archivujete na TAPE, IBM MQ se může rozšířit na maximálně 20 svazků.

Doporučené nastavení:

Testovací systém DASD

Produkční systém Páska

Další informace o výběru umístění pro protokoly archivace naleznete v příručce [Plánování v systému z/OS](#).

UNIT2

Uvádí typ zařízení nebo název jednotky zařízení, které se používá k uložení druhé kopie datových sad protokolu archivace.

Uvedte typ zařízení nebo název jednotky 1 až 8 alfanumerických znaků. První znak musí být písmeno. Je-li tento parametr prázdný, použije se hodnota nastavená pro parametr UNIT.

Výchozí hodnota je prázdná.

Související odkazy

“Použití CSQ6SYSP” na stránce 552

Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6SYSP.

“Použití CSQ6LOGP” na stránce 561

Toto téma použijte jako referenci, jak určit volby protokolování pomocí CSQ6LOGP.

Úloha 18: Přizpůsobte parametry inicializátoru kanálu

Pomocí příkazu ALTER QMGR můžete upravit inicializátor kanálu tak, aby vyhovoval vašim požadavkům.

- *Podle potřeby opakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Tuto úlohu musíte provést při migraci z předchozí verze.*

Řada atributů správce front řídí způsob, jakým jsou distribuované fronty spouštěny. Nastavte tyto atributy pomocí příkazu MQSC ALTER QMGR. Ukázka inicializační datové sady thlqual.SCSQPROC(CSQ4INYG) obsahuje některá nastavení, která lze přizpůsobit. Další informace viz [ALTER QMGR](#).

Hodnoty těchto parametrů se zobrazí jako série zpráv pokaždé, když spustíte inicializátor kanálu.

Vztah mezi adaptéry, dispečery a maximálním počtem kanálů

Parametry příkazu ALTER QMGR CHIADAPS a CHIDISPS definují počet řídicích bloků úloh (TCB) používaných inicializačním programem kanálu. CHIADAPS (adaptér) TCB se používají k vytvoření volání rozhraní API produktu IBM MQ do správce front. CHIDISPS (dispečer) TCB se používají pro volání do komunikační sítě.

Parametr ALTER QMGR MAXCHL ovlivňuje distribuci kanálů v rámci dispečerů TCB.

CHIDISPS

Máte-li malý počet kanálů, použijte výchozí hodnotu.

Jedna úloha pro každý procesor optimalizuje výkon systému. Vzhledem k tomu, že úlohy dispečeru jsou náročné na procesor, je třeba zachovat co nejméně málo úloh, aby byla minimalizována doba potřebná k vyhledání a spuštění podprocesů.

CHIDISPS (20) je vhodný pro systémy s více než 100 kanály. Je nepravděpodobné, že by došlo k významnému znevýhodnění v případě CHIDISPS (20), je-li to více dispečerů TCB, než je nezbytné.

Pokud máte více než 1000 kanálů, můžete povolit jeden dispečer pro každých 50 aktuálních kanálů. Například, uveďte CHIDISPS (40), chcete-li zpracovat až 2000 aktivních kanálů.

Pokud používáte protokol TCP/IP, je maximální počet dispečerů použitých pro kanály TCP/IP 100, a to i v případě, že v systému CHIDISPS zadáte větší hodnotu.

CHIADAPS

Každé volání rozhraní API produktu IBM MQ pro správce front je nezávislé na jiných systémech a lze je provést na libovolném adaptéru TCB. Volání používající trvalé zprávy mohou trvat mnohem déle, než je tomu u dočasných zpráv kvůli I/O protokolu. Proto může zpracování kanálu iniciátoru velkého počtu trvalých zpráv v rámci mnoha kanálů vyžadovat více než výchozí 8 adaptérů TCB pro optimální výkon. Je tomu tak zvláště tehdy, je-li velikost batchsize malá, protože zpracování dávkového zpracování také vyžaduje vstup/výstup protokolu a kde se používají kanály tenkého klienta.

Doporučená hodnota pro produkční prostředí je CHIADAPS (30). Použití více, než je nepravděpodobné, může poskytnout jakýkoli významný přínos navíc a je nepravděpodobné, že by byla jakákoliv významná nevýhoda v případě CHIADAPS (30), pokud se jedná o více TCB, než je nezbytné.

MAXCHL

Každý kanál je přidružen ke konkrétnímu dispečeru TCB při spuštění kanálu a zůstává přidružen k této TCB, dokud se kanál nezastaví. Každý TCB může sdílet mnoho kanálů. Hodnota MAXCHL se používá k šíření kanálů v rámci dostupných dispečerů TCB. První (MIN ((MAXCHL/CHIDISPS) , 10)) kanály, které se mají spustit, jsou přidruženy k prvnímu dispečeru TCB a tak dále, dokud se nebudou používat všechny dispečery TCB.

Dopad tohoto počtu na malý počet kanálů a velký MAXCHL je, že kanály nejsou rovnoměrně rozmístěny mezi dispečery. Pokud jste například nastavili CHIDISPS (10) a ponechal MAXCHL při výchozí hodnotě 200, ale měl pouze 50 kanálů, pět dispečerů by bylo asociováno s 10 kanály každý a pět by bylo nepoužité. Navrhujeme nastavení MAXCHL na počet kanálů, které se skutečně používají, kde se jedná o malé pevné číslo.

Změníte-li tuto vlastnost správce front, musíte také zkontrolovat vlastnosti správce front ACTCHL, LU62CHLa TCPCHL, abyste se ujistili, že jsou hodnoty kompatibilní. Úplný popis těchto vlastností a jejich vztah viz [Parametry správce front](#) .

Nastavení prostředí produktu z/OS UNIX System Services pro iniciátory kanálu

Inicializátor kanálu (CHINIT) používá podprocesy OMVS. Před vytvořením nové CHINIT nebo změnou počtu dispečerů nebo SSLTASKS zkontrolujte konfigurační parametry OMVS.

Každá CHINIT používá podprocesy 3 + CHIDISP + SSLTASKS OMVS. Tyto příspěvky přispívají k celkovému počtu podprocesů OMVS použitých v oblasti LPAR a k počtu podprocesů použitých ID uživatele spuštěných úloh CHINIT.

Můžete použít produkt **D OMVS, L** a zkontrolovat aktuální využití, využití vysoké vody a omezení systému MAXPROCSYS (maximální počet procesů, které systém povoluje).

Pokud přidáváte nové CHINIT nebo zvyšujete hodnoty parametrů CHIDISPS nebo SSLTASKS, musíte vypočítat nárůst podprocesů a zkontrolovat dopad na hodnoty MAXPROCSYS. Pomocí příkazu **SETOMVS** můžete dynamicky změnit hodnotu MAXPROCSYS nebo aktualizovat hodnotu parametru parmXPRCxx nebo obě.

Parametr OMVS MAXPROCUSER je počet vláken OMVS jednoho uživatele OMVS, který je se stejným UID, který může mít. Podprocesy se započítávají do této hodnoty. Takže pokud máte 2 CHINITs se stejným ID uživatele spuštěné úlohy, s 10 dispečery a 3 SSLTASKS, každý pak bude $2 * (3 + 10 + 3) = 32$ vláken pro UID OMVS.

Výchozí parametr MAXPROCUSER můžete zobrazit zadáním příkazu **D OMVS, O** a pomocí příkazu **SETOMVS** můžete dynamicky změnit hodnotu MAXPROCUSER nebo aktualizovat hodnotu parametru parmXPRCxx nebo obojí.

Tuto hodnotu můžete přepsat na bázi pro uživatele pomocí příkazu RACF **ALTUSER userid OMVS (PROCUSERMAX(nnnn))** nebo podobného.

Chcete-li spustit inicializátor kanálu, zadejte následující příkaz:

```
START CHINIT
```

Chcete-li se ujistit, že byl inicializátor kanálu úspěšně spuštěn, zkontrolujte, zda v protokolu úlohy xxxxCHIN(ssidCHIN) není chyba ICH408I .

Související pojmy

[“Úloha 19: Nastavení dávky, TSO a adaptérů RRS” na stránce 574](#)

Zpřístupněte adaptéry pro aplikace tím, že přidáte knihovny do příslušných zřetězení STEPLIB. Chcete-li obstarávat výpisy paměti SNAP vydané adaptérem, přiřadte jméno CSQSNAP DDname. Zvažte použití CSQBDEFV ke zlepšení přenositelnosti vašich aplikačních programů.

Související informace

[Záznamy dat statistiky inicializátoru kanálu](#)

Úloha 19: Nastavení dávky, TSO a adaptérů RRS

Zpřístupněte adaptéry pro aplikace tím, že přidáte knihovny do příslušných zřetězení STEPLIB. Chcete-li obstarávat výpisy paměti SNAP vydané adaptérem, přiřďte jméno CSQSNAP DDname. Zvažte použití CSQBDEFV ke zlepšení přenositelnosti vašich aplikačních programů.

- *Tuto úlohu opakujte pro každého správce front produktu IBM MQ podle potřeby.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Chcete-li zpřístupnit adaptéry pro dávkové a jiné aplikace pomocí dávkových připojení, přidejte do struktury STEPLIB pro vaši dávkovou aplikaci následující knihovny produktu IBM MQ :

- thlqual.SCSQANL x
- thlqual.SCSQAUTH

kde x je jazyková písmena pro váš národní jazyk. (Tuto akci nemusíte provádět, pokud jsou knihovny v LPA nebo seznamu odkazů.)

Pro aplikace TSO přidejte knihovny do zřetězení STEPLIB v přihlašovacím postupu TSO nebo pomocí příkazu TSO TSOLIB aktivujte tyto knihovny.

Pokud adaptér zjistí neočekávanou chybu IBM MQ , odešle výpis paměti z/OS SNAP na DDname CSQSNAP a vydá do aplikace kód příčiny MQRC_UNEXPECTED_ERROR .Pokud příkaz CSQSNAP DD není v aplikaci JCL nebo CSQSNAP není přidělen k datové sadě pod TSO, žádný výpis paměti nebude proveden. Pokud k tomu dojde, můžete zahrnout příkaz CSQSNAP DD do JCL aplikace nebo alokovat CSQSNAP k datové sadě pod TSO a znovu spustit aplikaci. Avšak protože některé problémy jsou občasné, doporučujeme vám zahrnout příkaz CSQSNAP do JCL aplikace nebo alokovat CSQSNAP k datové sadě v proceduře přihlášení TSO, abyste zachytili příčinu selhání v době, kdy k němu dojde.

Dodaný program CSQBDEFV zlepšuje přenositelnost vašich aplikačních programů. V CSQBDEFV můžete zadat název správce front nebo skupiny sdílení front, které mají být připojeny, než abyste ji zadali v rámci volání MQCONN nebo MQCONNX v aplikačním programu. Můžete vytvořit novou verzi CSQBDEFV pro každého správce front nebo skupinu sdílení front. Postupujte takto:

1. Okopírujte program IBM MQ assembler CSQBDEFV z thlqual.SCSQASMS do uživatelské knihovny.
2. Dodaný program obsahuje výchozí název subsystému CSQ1. Tento název můžete uchovat pro testování a verifikaci instalace. V případě produkčních subsystémů můžete změnit název NAME=CSQ1 na název subsystému se čtyřmi znaky nebo použít řetězec CSQ1.

Používáte-li skupiny sdílení front, můžete místo hodnoty CSQ1zadat název skupiny sdílení front. Pokud tak učiníte, program vydá žádost o připojení k aktivnímu správci front v rámci této skupiny.

3. Sestavte a propojte program za účelem získání zaváděcího modulu CSQBDEFV. Pro sestavení zahrňte knihovnu thlqual.SCSQMACS do zřetězení SYSLIB; použijte parametry linkování RENT ,AMODE=31 , RMODE=ANY. Tato hodnota je zobrazena v ukázkovém JCL v souboru thlqual.SCSQPROC(CSQ4DEFV). Poté zahrňte zaváděcí knihovnu do tabulky z/OS Batch nebo TSO STEPLIB před thlqual.SCSQAUTH.

Související pojmy

[“Úloha 20: Nastavení panelů operací a ovládacích panelů” na stránce 574](#)

Chcete-li nastavit operace a ovládací panely, musíte nejprve nastavit knihovny, které obsahují požadované panely, EXECs, zprávy a tabulky. Abyste to mohli udělat, musíte vzít v úvahu, která národní jazyková funkce se má používat pro panely. Po provedení této akce můžete volitelně aktualizovat hlavní nabídku ISPF pro operace IBM MQ a ovládací panely a měnit nastavení funkčních kláves.

Úloha 20: Nastavení panelů operací a ovládacích panelů

Chcete-li nastavit operace a ovládací panely, musíte nejprve nastavit knihovny, které obsahují požadované panely, EXECs, zprávy a tabulky. Abyste to mohli udělat, musíte vzít v úvahu, která národní jazyková

funkce se má používat pro panely. Po provedení této akce můžete volitelně aktualizovat hlavní nabídku ISPF pro operace IBM MQ a ovládací panely a měnit nastavení funkčních kláves.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Nastavení knihoven

Chcete-li nastavit operace IBM MQ a ovládací panely, postupujte takto:

1. Ujistěte se, že všechny knihovny obsažené ve vašich zřetězení jsou buď ve stejném formátu (F, FB, V, VB) a mají stejnou velikost bloku nebo jsou v pořadí zmenšujících se velikostí bloku. Jinak byste mohli mít problémy při pokusu o použití těchto panelů.
2. Zahrňte knihovnu thlqual.SCSQEXEC do zřetězení SYSEXEC nebo SYSPROC nebo ji aktivujte pomocí příkazu TSO ALTLIB. Tato knihovna, která je během instalace přidělena s formátem 80 záznamů s pevnou velikostí bloku, obsahuje požadované EXECs.
Je vhodnější umístit knihovnu do zřetězení SYSEXEC. Pokud jej však chcete vložit do SYSPROC, musí mít knihovna délku záznamu 80 bajtů.
3. Přidejte thlqual.SCSQAUTH a thlqual.SCSQANLx do procedury přihlášení TSO STEPLIB nebo ji aktivujte pomocí příkazu TSO TSOLIB, pokud není uveden v seznamu odkazů nebo v LPA.
4. Můžete buď trvale přidat knihovny panelů IBM MQ do nastavení knihovny ISPF, nebo je povolit dynamicky nastavit při použití panelů. Pro předchozí volbu je třeba provést následující kroky:
 - a. Zahrňte knihovnu obsahující operace a definice ovládacího panelu ve zřetězení ISPLLIB. Název je thlqual.SCSQPNLx, kde x je jazyková písmena pro váš národní jazyk.
 - b. Zahrňte knihovnu obsahující požadované tabulky ve zřetězení ISPTLIB. Název je thlqual.SCSQTBLx, kde x je jazyková písmena pro váš národní jazyk.
 - c. Zahrňte knihovnu obsahující požadované zprávy ve zřetězení ISPMLIB. Název je thlqual.SCSQMSGx, kde x je jazyková písmena pro váš národní jazyk.
 - d. Zahrňte knihovnu obsahující požadované zaváděcí moduly do zřetězení ISPLLIB. Název této knihovny je thlqual.SCSQAUTH.
5. Otestujte, že máte přístup k panelům panelů IBM MQ z panelu příkazového procesoru TSO. Toto je obvykle volba 6 v menu primární volby ISPF/PDF. Název EXEC, který spustíte, je CSQOREXX. Nejsou žádné parametry, které byste měli uvést, pokud jste trvale umístili knihovny produktu IBM MQ do vašeho nastavení ISPF jako v kroku 4. Pokud jste nepoužili, použijte následující:

```
CSQOREXX thlqual langletter
```

kde langletter je písmeno označující národní jazyk, který má být použit:

- C** Zjednodušená čínština
- E** U.S. angličtina (smíšená velikost písmen)
- F** Francouzština
- K** japonština
- U** U.S. Angličtina (velká písmena)

Aktualizace nabídky ISPF

Hlavní nabídku ISPF můžete aktualizovat, chcete-li povolit přístup k operacím produktu IBM MQ a k ovládacím panelům z ISPF. Požadované nastavení pro & ZSEL je:

```
CMD(%CSQOREXX thlqual langletter)
```

Informace o thlqual a langletter naleznete v kroku “5” na stránce 575.

Další informace naleznete v příručce z/OS: *ISPF Developer's Guide and Reference* .

Aktualizace funkčních kláves a nastavení příkazů

Běžné procedury ISPF můžete použít ke změně funkčních kláves a nastavení příkazů používaných panely. Identifikátor aplikace je CSQO.

To však *není* doporučeno, protože informace nápovědy nejsou aktualizovány tak, aby odrážely všechny provedené změny.

Související pojmy

“Úloha 21: Zahrnout člena formátování výpisu paměti IBM MQ” na stránce 576

Chcete-li mít možnost formátovat výpisy paměti IBM MQ pomocí Interaktivního systému řízení problémů (IPCS), musíte aktualizovat některé systémové knihovny.

Úloha 21: Zahrnout člena formátování výpisu paměti IBM MQ

Chcete-li mít možnost formátovat výpisy paměti IBM MQ pomocí Interaktivního systému řízení problémů (IPCS), musíte aktualizovat některé systémové knihovny.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Při migraci z předchozí verze je třeba provést tuto úlohu.*

Chcete-li mít možnost formátovat výpisy paměti IBM MQ pomocí systému IPCS (Interactive Problem Control System), zkopírujte datovou sadu thlqual.SCSQPROC(CSQ7IPCS) do SYS1.PARMLIB. Tuto datovou sadu byste neměli upravovat.

Pokud jste přizpůsobili proceduru TSO pro IPCS, thlqual.SCSQPROC(CSQ7IPCS) lze zkopírovat do libovolné knihovny v definici IPCSPARM. Podrobnosti o IPCSPARM najdete v příručce *Customization MVS IPCS Customization* .

Do zřetězení ISPLIB musíte také zahrnout knihovnu thlqual.SCSQPDLA .

Chcete-li vytvořit programy pro formátování výpisu paměti dostupné pro vaši relaci TSO nebo IPCS, musíte do zřetězení STEPLIB zahrnout také knihovnu thlqual.SCSQAUTH nebo ji aktivovat pomocí příkazu TSO TSOLIB (i v případě, že již je v seznamu odkazů nebo v LPA).

Související pojmy

“Úloha 22: Potlačit informační zprávy” na stránce 576

Systém IBM MQ může produkovat velké množství informačních zpráv. Můžete zabránit odeslání vybraných zpráv na konzolu nebo do protokolu pevné kopie.

Úloha 22: Potlačit informační zprávy

Systém IBM MQ může produkovat velké množství informačních zpráv. Můžete zabránit odeslání vybraných zpráv na konzolu nebo do protokolu pevné kopie.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*

Je-li systém IBM MQ intenzivně využíván, je při zastavování a spouštění mnoha kanálů odesláno velké množství informačních zpráv do konzoly z/OS a do protokolu hardcopy. Most produktu IBM MQ - IMS a správce vyrovnávacích pamětí mohou také produkovat velké množství informačních zpráv.

V případě potřeby můžete některé z těchto zpráv konzoly potlačit použitím seznamu zařízení pro zpracování zpráv produktu z/OS určeného členy MPFLSTxx produktu SYS1.PARMLIB. Zprávy, které uvedete, se stále objeví v protokolu hardcopy, ale ne na konzole.

Ukázka `thlqual.SCSQPROC(CSQ4MPFL)` uvádí navrhované nastavení pro MPFLSTxx. Další informace o parametru MPFLSTxx naleznete v příručce *MVS Initialization and Tuning Reference*.

Chcete-li potlačit vybrané informační zprávy v protokolu hardcopy, můžete použít instalační uživatelskou proceduru produktu z/OS IEAVMXIT. Pro požadované zprávy můžete nastavit následující bitové přepínače:

CTXTRDTM

Odstraňte zprávu.

Zpráva se nezobrazuje na konzolách nebo není protokolována v tištěné podobě.

CTXTESJL

Potlačit z protokolu úlohy.

Zpráva nevstupuje do protokolu úlohy JES.

CTXTNWTP

Neprovádět zpracování WTP.

Zpráva se neodešle na terminál TSO ani na datovou sadu systémové zprávy dávkové úlohy.

Poznámka:

1. Podrobné informace o ostatních parametrech najdete v dokumentaci k produktu [MVS Installation Exit](#).
2. Nedoporučuje se potlačit zprávy jiné než v navrženém seznamu potlačení, CSQ4MPFL.

Kromě toho můžete zadat další parametr:

EXCLMSG

Uvádí seznam zpráv, které mají být vyloučeny z jakéhokoli protokolu.

Zprávy v tomto seznamu se neodešlou do konzoly z/OS a do protokolu hardcopy. Další informace naleznete v části [EXCLMSG](#) v příručce [“Použití CSQ6SYSP”](#) na stránce 552.

Související pojmy

[“Testování správce front v systému z/OS”](#) na stránce 582

Pokud jste správce front přizpůsobili nebo provedli migraci, můžete jej otestovat spuštěním některých ukázkových aplikací dodávaných s produktem IBM MQ.

Úloha 23: Vytvořit procedury pro rozšířené zabezpečení zpráv

Každý subsystém IBM MQ, který má být konfigurován k použití produktu Advanced Message Security, vyžaduje ke spuštění adresního prostoru AMS katalogovou proceduru. Můžete vytvořit vlastní nebo použít knihovnu procedur dodané s produktem IBM.

Pro každý subsystém IBM MQ, který má být konfigurován pro použití produktu Advanced Message Security, si přizpůsobte kopii ukázkové procedury CSQ4AMSM. Chcete-li to provést, proveďte následující kroky:

1. Okopírujte ukázkovou proceduru spuštění úlohy `thlqual.SCSQPROC(CSQ4AMSM)` do vašeho SYS1.PROCLIB nebo, pokud nepoužíváte SYS1.PROCLIB, vaše knihovna procedur. Nazvěte proceduru `xxxxAMSM`, kde `xxxx` je název vašeho subsystému IBM MQ. Například `CSQ1AMSM` by byla procedura spuštěné úlohy AMS pro správce front CSQ1.
2. Vytvořte kopii pro každý subsystém IBM MQ, který budete používat.
3. Přizpůsobte si postupy podle pokynů uvedených v ukázkové proceduře CSQ4AMSM. Symbolické parametry v souboru JCL můžete také použít k povolení úpravy procedury při jeho spuštění.

4. Zkontrolujte a případně změňte parametry předávané úloze AMS pomocí souboru Language Environment® _CEE_ENVFILE. Ukázka thlqual.SCSQPROC(CSQ40ENV) obsahuje seznam podporovaných parametrů.

Poznámka: Tato úloha by měla být opakována pro každého správce front IBM MQ .

Úloha 24: Nastavit zabezpečení rozšířených zpráv spuštěné úlohy uživatele

Úloha IBM MQ Advanced Message Security vyžaduje ID uživatele, které mu umožňuje být známý jako proces služeb systému UNIX .

Kromě toho uživatelé, kterým úloha pracuje, musí mít také odpovídající definici UNIX UID (ID uživatele) a GID (ID skupiny), takže tito uživatelé jsou známí jako uživatelé produktu UNIX System Services. Další informace o definování identifikátorů UID a GID služeb UNIX System Services viz příručka *z/OS: Security Server RACF Security Administrator's Guide*.

Produkt *z/OS: UNIX System Services Planning* porovnává tradiční zabezpečení produktu UNIX se zabezpečením produktu *z/OS* . Primární rozdíl mezi tradičním zabezpečením produktu UNIX a zabezpečením produktu *z/OS* spočívá v tom, že služby jádra podporují dvě úrovně odpovídajících oprávnění: úroveň UNIX a úroveň *z/OS* UNIX .

V závislosti na zásadách zabezpečení instalace může být úloha IBM MQ Advanced Message Security spuštěna buď s oprávněním superuživatele (uid (0)), nebo se svou identitou RACF povolenou pro třídu FACILITY RACF BPX.DAEMON a BPX.SERVER , protože tato úloha musí být schopna převzít identitu RACF svých uživatelů.

Je-li použita druhá metoda, nebo jste již aktivovali BPX.DAEMON nebo BPX.SERVER , program úlohy IBM MQ Advanced Message Security (thlqual.SCSQAUTH(CSQ0DSRV)) musí být umístěn v knihovnách řízených programem RACF .

Zkontrolujte produkt *z/OS: UNIX System Services Planning* a ujistěte se, že rozumíte bezpečnostním rozdílům mezi tradičním zabezpečením produktu UNIX a zabezpečením produktu *z/OS* UNIX . To vám umožní spravovat úlohu IBM MQ Advanced Message Security podle zásady zabezpečení vaší instalace pro implementaci a spuštění privilegovaných procesů služeb systému UNIX .

Pro referenční účely jsou publikace užitečné pro tento přezkum:

- *z/OS: UNIX Plánování systémových služeb*.
- *z/OS: Security Server RACF Security Administrator's Guide*.

Poznámka: Zvolte ID uživatele pro tuto úlohu opatrně, protože certifikáty příjemce produktu IBM MQ Advanced Message Security se načtou do svazku klíčů přidruženého k tomuto ID uživatele. Tato úvaha je diskutována v tématu [Použití certifikátů v systému z/OS](#) .

Zde uvedené kroky popisují, jak nastavit uživatele spuštěné úlohy produktu IBM MQ Advanced Message Security . Tyto kroky používají jako příklady příkazy RACF . Používáte-li jiného správce zabezpečení, měli byste použít ekvivalentní příkazy.

Poznámka: Příklady v této sekci předpokládají, že jste aktivovali zpracování příkazu generického profilu pro třídy RACF STARTED, FACILITY, SURROGAT a kontrolu generických profilů. Další informace o tom, jak produkt RACF zachází s generickými profily, najdete v tématu *z/OS: Security Server RACF Command Language Reference*.

1. Nejprve nadefinujte uživatelské profily produktu RACF pro uživatele spuštěné úlohy produktu IBM MQ Advanced Message Security . Mohou to být stejní uživatelé.

```
ADDUSER WMQAMSM NAME('IBM MQ Advanced Message Security user') OMVS (UID(0)) DFLTGRP(group)
```

Vyberte výchozí 'skupinu', která odpovídá vašim instalačním standardům.

Poznámka: Pokud nechcete udělit oprávnění uživatele USS superuživatele (UID (0)), musíte povolit ID uživatele produktu IBM MQ Advanced Message Security pro objekt BPX.DAEMON a BPX.SERVER profily třídy zařízení:

```
PERMIT BPX.DAEMON CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
```

a program úlohy IBM MQ Advanced Message Security (*thlqual.SCSQAUTH* (CSQ0DSRV)) musí být umístěn v knihovně řízené programem RACF .

Chcete-li nastavit kontrolovaný program knihovny SCSQAUTH, můžete použít následující příkaz:

```
RALTER PROGRAM * ADDMEM('thlqual.SCSQAUTH'//NOPADCHK) -or-  
RALTER PROGRAM ** ADDMEM('thlqual.SCSQAUTH'//NOPADCHK)  
SETROPTS WHEN(PROGRAM) REFRESH
```

Musíte také povolit řízení programu pro národní jazykovou knihovnu (*thlqual.SCSQANLx*), která je použita úlohou IBM MQ Advanced Message Security .

2. Určete, zda je třída RACF STARTED aktivní. Pokud není, aktivujte třídu STARTED RACF STARTED:

```
SETROPTS CLASSACT(STARTED)
```

3. Definujte profil spuštěné třídy pro úlohy produktu IBM MQ Advanced Message Security zadáním ID uživatelů, které jste vybrali nebo jste vytvořili v kroku 1:

```
RDEFINE STARTED qmgr AMSM.* STDATA(USER(WMQAMSM))
```

kde *qmgr* je název předpony spuštěného názvu úlohy. Spuštěné úlohy mohou mít například název CSQ1AMSM. V tomto případě byste nahradil *qmgr* AMSM.* pomocí CSQ1AMSM.*.

Názvy spuštěných úloh musí mít název *qmgr* AMSM.*.

4. Pomocí příkazu SETROPTS RACF obnovte profily spuštěných tříd RACLISTed pro ukládání dat v úložišti:

```
SETROPTS RACLIST(STARTED) REFRESH
```

5. Úloha IBM MQ Advanced Message Security dočasně přebírá identitu ID uživatele hostitele žadatele během zpracování ochrany zpráv produktu IBM MQ . Proto je nezbytné definovat profily ve třídě SURROGAT pro každé ID uživatele, které může vytvářet požadavky.

To lze provést s jedním generickým profilem, je-li třída SURROGAT RACF aktivní. Tato kontrola je ignorována, pokud třída SURROGAT není aktivní. Potřebné profily SURROGAT jsou popsány v příručce z/OS: *UNIX System Services Planning*.

Chcete-li definovat profily ve třídě SURROGAT:

- a. Třídu SURROGAT produktu RACF aktivujte pomocí příkazu RACF SETROPTS:

```
SETROPTS CLASSACT(SURROGAT)
```

- b. Aktivace zpracování generických profilů pro třídu RACF SURROGAT:

```
SETROPTS GENERIC(SURROGAT)
```

- c. Aktivace zpracování příkazu generického profilu pro třídu RACF SURROGAT:

```
SETROPTS GENCMD(SURROGAT)
```

- d. Definujte generický profil náhradní třídy:

```
RDEFINE SURROGAT BPX.SRV.* UACC(NONE)
```

- e. Povolte ID uživatele produktu IBM MQ Advanced Message Security do generického profilu třídy SURROGAT:

```
PERMIT BPX.SRV.* CLASS(SURROGAT) ID(WMQAMSM) ACCESS(UPDATE)
```

Poznámka: Můžete definovat více specifických profilů, chcete-li omezit určité uživatele, které mají být zpracovány úlohou IBM MQ Advanced Message Security, jak je popsáno v *z/OS: UNIX Plánování služeb systému*.

- f. Povolte ID uživatele produktu IBM MQ Advanced Message Security k prostředku BPX.SERVER (pokud již není provedeno v části [Vytvoření certifikátů a klíčových řetězců](#)):

```
PERMIT BPX.SERVER CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
```

6. Úloha produktu IBM MQ Advanced Message Security používá funkce poskytované službami z/OS System SSL k otevření klíčových kruhů spravovaných zařízeními SAF. Nástroj SAF (System Authorization Facility), který přistupuje k obsahu svazků klíčů, je řízen produktem RACF nebo ekvivalentním správcem zabezpečení.

Tato služba je volatelnou službou IRRSDL00 (R_datalib). Tato volatelná služba je chráněna stejnými profily, které se používají k ochraně příkazů RACF RACDCERT, které jsou definovány pro třídu FACILITY RACF. ID uživatele produktu IBM MQ Advanced Message Security proto musí být povoleno pro profily pomocí těchto příkazů:

- a. Pokud jste tak dosud neučinili, definujte generický profil produktu RACF pro třídu FACILITY produktu RACF, která chrání příkaz RACDCERT a volatelnou službu IRRSDL00:

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)  
SETROPTS RACLIST(FACILITY) REFRESH
```

- b. Udělte oprávnění ke spouštěným ID uživatele úlohy do generického profilu RACF:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(WMQAMSM) ACC(READ)
```

Případně můžete do třídy RDATA LIB udělit přístup pro čtení ke svazku klíčů uživatele úlohy datové služby, jak je uvedeno níže:

```
PERMIT WMQASMD.DRQ.AMS.KEYRING.LST CLASS(RDATA LIB) ID(WMQAMSM) ACC(READ)
```

Zabezpečení prostředků pro AMS

Uživatel spuštěné úlohy vyžaduje oprávnění ke čtení pro SYSTEM.PROTECTION.POLICY.QUEUE.

Uživatel se spuštěnou úlohou vyžaduje oprávnění k připojení ke správci front jako aplikace BATCH. Další informace naleznete v tématu [Profily zabezpečení připojení pro dávkové připojení](#).

Úloha 25: Udělení oprávnění RACDCERT správci zabezpečení pro rozšířenou bezpečnost zpráv

Administrátor zabezpečení produktu IBM MQ Advanced Message Security vyžaduje oprávnění k použití příkazu RACDCERT pro vytváření a správu digitálních certifikátů.

Identifikujte odpovídající ID uživatele pro tuto roli a udělte oprávnění pro použití příkazu RACDCERT.
Příklad:

```
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID(admin) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

kde `admin` je ID uživatele vašeho administrátora zabezpečení produktu IBM MQ Advanced Message Security .

Úloha 26: Udělení oprávnění k prostředkům uživatelům pro produkt IBM MQ Advanced Message Security

Uživatelé produktu IBM MQ Advanced Message Security vyžadují příslušná oprávnění k prostředkům.

Uživatelé IBM MQ Advanced Message Security , kteří jsou uživateli, kteří vkládají nebo dostávají IBM MQ Advanced Message Security chráněné zprávy, vyžadují:

- Segment OMVS přidružený k jejich ID uživatele
- Oprávnění pro IRR.DIGTCERT.LISTRING nebo RDATA LIB
- Oprávnění pro profily CSFSERV a CSFKEYS třídy ICSF

Úloha IBM MQ Advanced Message Security dočasně přebírá identitu svých klientů; to znamená, že úloha se chová jako náhrada ID uživatele z/OS uživatelů produktu IBM MQ Advanced Message Security během zpracování zpráv produktu IBM MQ do front, které jsou chráněny produktem IBM MQ Advanced Message Security.

Má-li úloha převzít identitu z/OS uživatele, musí mít ID uživatele klienta z/OS definovaný segment OMVS, který je přidružen k jeho uživatelskému profilu.

Jako administrativní pomůcka poskytuje produkt RACF možnost definovat výchozí segment OMVS, který může být přidružen k uživatelským a skupinovým profilům RACF . Tato předvolba se použije, pokud ID uživatele nebo profil skupiny produktu z/OS nemá explicitně definovaný segment OMVS. Pokud plánujete mít velký počet uživatelů pomocí produktu IBM MQ Advanced Message Security, můžete se rozhodnout použít tuto výchozí hodnotu, místo abyste výslovně definovali segment OMVS pro každého uživatele.

Příručka *z/OS: Security Server RACF Security Administrator's Guide* obsahuje podrobný postup pro definování výchozích segmentů OMVS. Projděte si proceduru popsanou v této příručce a určete, zda je definice výchozích segmentů OMVS v profilech uživatele a skupiny produktu RACF vhodná pro vaši instalaci.

Chcete-li udělit oprávnění READ pro IRR.DIGTCERT.LISTRING zařízení třídy pro všechny uživatele IBM MQ Advanced Message Security , zadejte tento příkaz:

```
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(READ)
```

nebo udělte oprávnění READ pro jednotlivé uživatele zadáním tohoto příkazu:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(userid) ACCESS(READ)
```

kde `ID` uživatele je jméno uživatele IBM MQ Advanced Message Security .

Případně můžete použít třídu RDATA LIB k udělení přístupu k určitým klíčovým klíčům (oprávnění RDATA LIB mají přednost před hodnotou IRR.DIGTCERT.LISTRING oprávnění). Příklad:

```
PERMIT user.DRQ.AMS.KEYRING.LST CLASS(RDATA LIB) ID(user) ACC(READ)
```

Používáte-li certifikáty správy ICSF a soukromé klíče, vyžadují uživatelé produktu IBM MQ Advanced Message Security přístup k určitým profilům CSFSERV a CSFKEYS. Tento přístup je podrobně popsán v následující tabulce:

Tabulka 46. Požadovaný uživatelský přístup k profilům CSFSERV a CSFKEYS

Třída	Profil	Oprávnění
CSFSERV	CSFDSG	READ (čtení)
CSFSERV	CSFPKE	READ (čtení)
CSFSERV	CSFPKD	READ (čtení)
CSFSERV	CSFDSV	READ (čtení)
KLÍČE CSFKEYS	Návěští ICSF PKDS	READ (čtení)

Testování správce front v systému z/OS

Pokud jste správce front přizpůsobili nebo provedli migraci, můžete jej otestovat spuštěním některých ukázkových aplikací dodávaných s produktem IBM MQ.

Můžete kompilovat a upravit odkaz-upravit podle toho, která z dalších ukázek je pro vaši instalaci vhodná s použitím ukázkového souboru JCL.

Pokyny týkající se způsobu testování správce front v systému z/OS: naleznete v následujících odkazech.

- [“Spuštění programu pro ověření základní instalace”](#) na stránce 582
- [“Testování skupin sdílení front”](#) na stránce 586
- [“Testování distribuovaných front”](#) na stránce 587
- [“Testování pro jazyky C, C + +, COBOL, PL/I a CICS”](#) na stránce 590

Související pojmy

[“Konfigurace správců front v systému z/OS”](#) na stránce 523

Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Související informace

[IBM MQ for z/OS koncepce](#)

[Plánování vašeho prostředí IBM MQ na systému z/OS](#)

[Správa serveru IBM MQ for z/OS](#)

Spuštění programu pro ověření základní instalace

Po instalaci a přizpůsobení produktu IBM MQ můžete použít dodaný program pro ověření instalace CSQ4IVP1, abyste potvrdili, že je produkt IBM MQ funkční.

Základní program pro ověření instalace je dávkovým kompilátorem IVP, který ověřuje základní soubor IBM MQ bez použití ukázek C, COBOL nebo CICS .

Modul IVP produktu Batch Assembler IVP je upraven nástrojem SMP/E a moduly načtení jsou dodávány v knihovně thlqual.SCSQLOAD.

Po dokončení kroku SMP/E APPLY a kroků přizpůsobení spusťte program IVP produktu Batch Assembler IVP.

Další podrobnosti naleznete v těchto oddílech:

- [Přehled aplikace CSQ4IVP1](#)
- [Příprava na spuštění CSQ4IVP1](#)
- [Spuštění CSQ4IVP1](#)
- [Kontrola výsledků CSQ4IVP1](#)

Přehled aplikace CSQ4IVP1

CSQ4IVP1 je dávková aplikace, která se připojuje k subsystému IBM MQ a provádí tyto základní funkce:

- Vydá volání IBM MQ
- Komunikuje s příkazovým serverem
- Ověřuje, zda je spuštění aktivní
- Generuje a odstraní dynamickou frontu
- Ověřuje zpracování ukončení platnosti zprávy.
- Ověřuje zpracování potvrzení zprávy

Příprava na spuštění CSQ4IVP1

Před spuštěním příkazu CSQ4IVP1:

1. Zkontrolujte, zda se položky IVP nacházejí ve zřetězení datové sady CSQINP2 ve spouštěcím programu správce front. Položky IVP se dodávají v členu thlqual.SCSQPROC(CSQ4IVPQ). Pokud tomu tak není, přidejte do své zřetězení CSQINP2 definice uvedené v souboru thlqual.SCSQPROC(CSQ4IVPQ). Je-li správce front momentálně spuštěn, je třeba jej restartovat, aby se tyto definice mohly projevit.
2. Ukázkový kód JCL CSQ4IVPR, který je vyžadován ke spuštění ověřovacího programu instalace, je v knihovně thlqual.SCSQPROC.

Upravte soubor JCL CSQ4IVPR s kvalifikátorem vyšší úrovně pro knihovny produktu IBM MQ , národní jazyk, který chcete použít, čtyřznakový název správce front produktu IBM MQ a místo určení pro výstup úlohy.

3. Aktualizujte produkt RACF tak, aby byl produkt CSQ4IVP1 povolen pro přístup k jeho prostředkům, je-li zabezpečení produktu IBM MQ aktivní.

Chcete-li spustit CSQ4IVP1 , je-li zabezpečení produktu IBM MQ povoleno, potřebujete ID uživatele produktu RACF s oprávněním pro přístup k objektům. Podrobné informace o definování prostředků pro produkt RACF naleznete v tématu Nastavení zabezpečení v systému z/OS . ID uživatele, který spouští IVP, musí mít následující přístupové oprávnění:

Oprávnění	Profil	Třída
READ (čtení)	ssid.DISPLAY.PROCESS	MQCMDS
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.REPLY.MODEL	MQQUEUE
AKTUALIZOVAT	ssid.CSQ4IVP1.**	MQQUEUE
READ (čtení)	ssid.BATCH	MQCONN

Tyto požadavky předpokládají, že zabezpečení produktu IBM MQ je aktivní. Příkazy RACF pro aktivaci zabezpečení produktu IBM MQ jsou zobrazeny v Obrázek 91 na stránce 584. Tento příklad předpokládá, že název správce front je CSQ1 a že ID uživatele, který spouští ukázkou CSQ4IVP1 , je TS101.

```

RDEFINE MQCMDS CSQ1.DISPLAY.PROCESS
PERMIT CSQ1.DISPLAY.PROCESS CLASS(MQCMDS) ID(TS101) ACCESS(READ)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.INPUT
PERMIT CSQ1.SYSTEM.COMMAND.INPUT CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.REPLY.MODEL
PERMIT CSQ1.SYSTEM.COMMAND.REPLY.MODEL CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.CSQ4IVP1.**
PERMIT CSQ1.CSQ4IVP1.** CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQCONN CSQ1.BATCH
PERMIT CSQ1.BATCH CLASS(MQCONN) ID(TS101) ACCESS(READ)

```

Obrázek 91. Příkazy RACF pro CSQ4IVP1

Spuštění CSQ4IVP1

Pokud jste tyto kroky provedli, spusťte správce front. Je-li správce front již spuštěn a vy jste změnili CSQINP2, musíte správce front zastavit a restartovat jej.

Proces IVP se spouští jako dávková úloha. Upravte zakázkový list tak, aby odpovídal požadavkům na odeslání vaší instalace.

Kontrola výsledků CSQ4IVP1

IVP se dělí do 10 etap; každá fáze musí být dokončena s kódem dokončení nula, než se spustí další fáze. IVP generuje sestavu, vypisuje:

- Název správce front, ke kterému je připojen.
- Jedna jednořádková zpráva zobrazující kód dokončení a kód příčiny vrácený z každé fáze.
- Informační zpráva jednosměrně tam, kde je to vhodné.

Ukázková sestava je k dispozici v produktu [Obrázek 92 na stránce 586](#)

Vysvětlení kódů dokončení a příčin najdete v tématu [Zprávy, vyplnění a kódy příčiny produktu IBM MQ for z/OS](#).

Některé fáze mají více než jedno volání IBM MQ a v případě selhání je vydána zpráva označující specifické volání IBM MQ, které selhalo. Také v některých fázích IVP předkládá vysvětlující a diagnostické informace do pole komentáře.

Úloha IVP požaduje výlučnou kontrolu určitých objektů správce front, a proto by měla být jedním vláknem přes systém. Počet případů, kdy může být IVP spuštěn pro správce front, však není omezen.

Mezi funkce prováděné jednotlivými fázemi patří:

Fáze 1

Připojte se ke správci front zadáním volání rozhraní API MQCONN .

Fáze 2

Určete název vstupní fronty systémových příkazů, kterou používá příkazový server k načtení zpráv vzniklých při zpracování požadavku. Tato fronta přijímá požadavky na zobrazení z fáze 5.

Chcete-li to provést, posloupnost volání je:

1. Vydejte volání MQOPEN zadáním názvu správce front, abyste otevřeli objekt správce front.
2. Vydejte volání MQINQ, abyste vyhledali název vstupní fronty systému příkazů.
3. Vydejte volání MQINQ, abyste zjistili informace o různých přepínačích událostí správce front.
4. Vydejte volání MQCLOSE, abyste zavřeli objekt správce front.

Při úspěšném dokončení této fáze se v poli pro komentář zobrazí název vstupní fronty příkazu systému.

Fáze 3

Otevřete inicializační frontu pomocí voláníMQOPEN.

Tato fronta je otevřena v této fázi v očekávání zprávy spouštěče, která je doručena jako výsledek příkazového serveru, který odpovídá na požadavek z fáze 5. Fronta musí být otevřena pro vstup tak, aby splňovala kritéria spouštěče.

Fáze 4

Vytvořte trvalou dynamickou frontu pomocí volby CSQ4IVP1.MODEL fronta jako model. Dynamická fronta má stejné atributy jako model, ze kterého byla vytvořena. To znamená, že když jsou odpovědi z požadavku na příkazový server ve fázi 5 zapsány do této fronty, do inicializační fronty otevřené ve fázi 3 se zapíše zpráva spouštěče.

Po úspěšném dokončení této fáze je název trvalé dynamické fronty označen v poli komentáře.

Fáze 5

Vydejte požadavek MQPUT1 na frontu příkazů příkazového serveru.

Zpráva typu MQMT_REQUEST je zapsána do vstupní fronty systémových příkazů požadující zobrazení procesu CSQ4IVP1. Deskriptor zprávy pro zprávu určuje trvalou dynamickou frontu vytvořenou ve fázi 4 jako frontu pro odpověď pro odezvu příkazového serveru.

Fáze 6

Vydejte požadavek **MQGET** z inicializační fronty. V této fázi se na inicializační frontě otevřené ve fázi 3 vydá příkaz GET WAIT s intervalem 1 minuta. Očekává se, že vrácená zpráva bude zprávou spouštěče generovanou ve zprávách odezvy příkazového serveru, které jsou zapisovány do fronty pro odpověď.

Fáze 7

Odstraňte trvalou dynamickou frontu vytvořenou ve fázi 4. Vzhledem k tomu, že fronta stále obsahuje zprávy, je použita volba MQCO_PURGE_DELETE.

Fáze 8

1. Otevřete dynamickou frontu.
2. MQPUT zprávu s nastaveným intervalem vypršení platnosti.
3. Čekejte, až zpráva vyprší.
4. Pokuste se o příkaz MQGET s prošlou zprávou
5. Fronta MQCLOSE. Fronta.

Fáze 9

1. Otevřete dynamickou frontu.
2. MQPUT a message.
3. Vydejte MQCMIT k potvrzení aktuální jednotky práce.
4. Zpráva MQGET.
5. Chcete-li tuto zprávu vrátit zpět, zadejte příkaz MQBACK.
6. ZMQGET stejnou zprávu a ujistěte se, že počet vrácení je nastaven na 1.
7. Chcete-li zavřít frontu, zadejte příkaz MQCLOSE.

Fáze 10

Odpojte se od správce front pomocí příkazu MQDISC .

Po spuštění produktu IVP můžete odstranit všechny objekty, které již nepotřebujete.

Pokud se IVP nespustí úspěšně, vyzkoušejte každý krok ručně, abyste zjistili, která funkce selhala.

Tyto požadavky předpokládají, že zabezpečení produktu IBM MQ je aktivní. Příkazy RACF pro aktivaci zabezpečení produktu IBM MQ jsou zobrazeny v [Obrázek 93 na stránce 587](#). Tento příklad předpokládá, že název správce front je CSQ1 a že ID uživatele, který spouští ukázkou CSQ4IVP1, je TS101.

```
RDEFINE MQQUEUE CSQ1.CSQ4IVPG.**
PERMIT CSQ1.CSQ4IVPG.** CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)
```

Obrázek 93. Příkazy RACF pro CSQ4IVP1 pro skupinu sdílení front

Spuštění CSQ4IVP1 pro skupinu sdílení front

Pokud jste tyto kroky provedli, spusťte správce front. Je-li správce front již spuštěn a vy jste změnili CSQINP2, musíte správce front zastavit a restartovat jej.

Proces IVP se spouští jako dávková úloha. Upravte zakázkový list tak, aby odpovídal požadavkům na odeslání vaší instalace.

Kontrola výsledků CSQ4IVP1 pro skupinu sdílení front

IVP pro skupiny sdílení front funguje stejným způsobem jako základní IVP, až na to, že fronty, které se vytvoří, se nazývají CSQIVPG. xx. Chcete-li zkontrolovat výsledky IVP pro skupiny sdílení front, postupujte podle pokynů v příručce [“Kontrola výsledků CSQ4IVP1”](#) na stránce 584.

Testování distribuovaných front

Dodaný program pro ověření instalace CSQ4IVPX můžete použít k potvrzení, že distribuované fronty jsou v provozu.

Přehled úloh CSQ4IVPX

CSQ4IVPX je dávková úloha, která spouští inicializátor kanálu a vydává příkaz IBM MQ DISPLAY CHINIT. Tím je ověřeno, že všechny hlavní aspekty distribuovaných front jsou funkční a zároveň se vyhýbá potřebě nastavení definic kanálů a sítí.

Příprava na spuštění CSQ4IVPX

Před spuštěním skriptu CSQ4IVPX:

1. Ukázkový kód JCL CSQ4IVPX, který se požaduje ke spuštění ověřovacího programu instalace, je v knihovně thlqual.SCSQPROC.
Upravte soubor JCL CSQ4IVPX s kvalifikátorem vyšší úrovně pro knihovny produktu IBM MQ, národní jazyk, který chcete použít, název správce front se čtyřmi znaky a místo určení pro výstup úlohy.
2. Aktualizujte produkt RACF tak, aby byl produkt CSQ4IVPX povolen pro přístup k jeho prostředkům, je-li zabezpečení produktu IBM MQ aktivní. Chcete-li spustit CSQ4IVPX, je-li zabezpečení produktu IBM MQ povoleno, potřebujete ID uživatele produktu RACF s oprávněním pro přístup k objektům. Podrobné informace o definování prostředků pro produkt RACF naleznete v tématu [Nastavení zabezpečení v systému z/OS](#). ID uživatele, který spouští IVP, musí mít následující přístupové oprávnění:

Oprávnění	Profil	Třída
CONTROL	ssid.START.CHINIT a ssid.STOP.CHINIT	MQCMDS
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CSQUTIL.*	MQQUEUE

Oprávnění	Profil	Třída
READ (čtení)	ssid.BATCH	MQCONN
READ (čtení)	ssid.DISPLAY.CHINIT	MQCMDS

Tyto požadavky předpokládají, že je definován profil zabezpečení připojení ssid.CHIN (jak ukazuje Profily zabezpečení připojení pro iniciátor kanálu) a že je aktivní zabezpečení produktu IBM MQ . Příkazy RACF , které se mají provést, jsou zobrazeny v [Obrázek 94 na stránce 589](#). Tento příklad předpokládá:

- Název správce front je CSQ1 .
 - ID uživatele, který spouští ukázkou CSQ4IVPX je TS101
 - Adresní prostor inicializátoru kanálu je spuštěn pod ID uživatele CSQ1MSTR .
3. Aktualizujte produkt RACF tak, aby umožňoval adresní prostoru inicializátoru kanálu následující oprávnění k přístupu:

Oprávnění	Profil	Třída
READ (čtení)	ssid.CHIN	MQCONN
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CHANNEL.INITQ	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CHANNEL.SYNCQ	MQQUEUE
ALTER	ssid.SYSTEM.CLUSTER.COMMAND.QUEUE	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CLUSTER.TRANSMIT.QUEUE	MQQUEUE
ALTER	ssid.SYSTEM.CLUSTER.REPOSITORY.QUEUE	MQQUEUE
CONTROL	ssid.CONTEXT.**	MQADMIN

Příkazy RACF se také zobrazí v [Obrázek 94 na stránce 589](#).

```

RDEFINE MQCMDS CSQ1.DISPLAY.DQM
PERMIT CSQ1.DISPLAY.DQM CLASS(MQCMDS) ID(TS101) ACCESS(READ)

RDEFINE MQCMDS CSQ1.START.CHINIT
PERMIT CSQ1.START.CHINIT CLASS(MQCMDS) ID(TS101) ACCESS(CONTROL)

RDEFINE MQCMDS CSQ1.STOP.CHINIT
PERMIT CSQ1.STOP.CHINIT CLASS(MQCMDS) ID(TS101) ACCESS(CONTROL)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.INPUT
PERMIT CSQ1.SYSTEM.COMMAND.INPUT CLASS(MQQUEUE) ID(TS101,CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CSQUTIL.*
PERMIT CSQ1.SYSTEM.CSQUTIL.* CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQCONN CSQ1.BATCH
PERMIT CSQ1.BATCH CLASS(MQCONN) ID(TS101) ACCESS(READ)

RDEFINE MQCONN CSQ1.CHIN
PERMIT CSQ1.CHIN CLASS(MQCONN) ID(CSQ1MSTR) ACCESS(READ)

RDEFINE MQQUEUE CSQ1.SYSTEM.CHANNEL.SYNCQ
PERMIT CSQ1.SYSTEM.CHANNEL.SYNCQ CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.COMMAND.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.COMMAND.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(ALTER)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.TRANSMIT.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.TRANSMIT.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.REPOSITORY.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.REPOSITORY.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(ALTER)

RDEFINE MQQUEUE CSQ1.SYSTEM.CHANNEL.INITQ
PERMIT CSQ1.SYSTEM.CHANNEL.INITQ CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQADMIN CSQ1.CONTEXT.**
PERMIT CSQ1.CONTEXT.** CLASS(MQADMIN) ID(CSQ1MSTR) ACCESS(CONTROL)

```

Obrázek 94. Příkazy RACF pro CSQ4IVPX

Spuštění CSQ4IVPX

Pokud jste tyto kroky provedli, spusťte správce front.

Proces IVP se spouští jako dávková úloha. Upravte zakázkový list tak, aby odpovídal požadavkům na odeslání vaší instalace.

Kontrola výsledků CSQ4IVPX

CSQ4IVPX spustí obslužný program CSQUTIL IBM MQ , aby vydal tři příkazy MQSC. Datová sada výstupu SYSPRINT by měla vypadat jako [Obrázek 95](#) na stránce 590, ačkoli podrobnosti se mohou lišit v závislosti na attributech správce front.

- Měli byste se podívat na příkazy **(1)** , za kterými následuje několik zpráv.
- Poslední zpráva z každého příkazu by měla být "CSQ9022I ... NORMÁLNÍ DOKONČENÍ" **(2)**.
- Úloha jako celek by měla být dokončena s návratovým kódem nula **(3)**.

```

CSQU000I CSQUTIL IBM MQ for z/OS - V6
CSQU001I CSQUTIL Queue Manager Utility - 2005-05-09 09:06:48
COMMAND
CSQU127I CSQUTIL Executing COMMAND using input from CSQUCMD data set
CSQU120I CSQUTIL Connecting to queue manager CSQ1
CSQU121I CSQUTIL Connected to queue manager CSQ1
CSQU055I CSQUTIL Target queue manager is CSQ1
START CHINIT
(1)
CSQN205I COUNT= 2, RETURN=00000000, REASON=00000004
CSQM138I +CSQ1 CSQMSCHI CHANNEL INITIATOR STARTING
CSQN205I COUNT= 2, RETURN=00000000, REASON=00000000
CSQ9022I +CSQ1 CSQXCRPS ' START CHINIT' NORMAL COMPLETION
(2)
DISPLAY CHINIT
(1)
CSQN205I COUNT= 2, RETURN=00000000, REASON=00000004
CSQM137I +CSQ1 CSQMDDQM DISPLAY CHINIT COMMAND ACCEPTED
CSQN205I COUNT= 12, RETURN=00000000, REASON=00000000
CSQX830I +CSQ1 CSQXRQDM Channel initiator active
CSQX002I +CSQ1 CSQXRQDM Queue-sharing group is QSG1
CSQX831I +CSQ1 CSQXRQDM 8 adapter subtasks started, 8 requested
CSQX832I +CSQ1 CSQXRQDM 5 dispatchers started, 5 requested
CSQX833I +CSQ1 CSQXRQDM 0 SSL server subtasks started, 0 requested
CSQX840I +CSQ1 CSQXRQDM 0 channel connections current, maximum 200
CSQX841I +CSQ1 CSQXRQDM 0 channel connections active, maximum 200,
including 0 paused
CSQX842I +CSQ1 CSQXRQDM 0 channel connections starting,
0 stopped, 0 retrying
CSQX836I +CSQ1 Maximum channels - TCP/IP 200, LU 6.2 200
CSQX845I +CSQ1 CSQXRQDM TCP/IP system name is TCPIP
CSQX848I +CSQ1 CSQXRQDM TCP/IP listener INDISP=QMGR not started
CSQX848I +CSQ1 CSQXRQDM TCP/IP listener INDISP=GROUP not started
CSQX849I +CSQ1 CSQXRQDM LU 6.2 listener INDISP=QMGR not started
CSQX849I +CSQ1 CSQXRQDM LU 6.2 listener INDISP=GROUP not started
CSQ9022I +CSQ1 CSQXCRPS ' DISPLAY CHINIT' NORMAL COMPLETION
(2)
STOP CHINIT
(1)
CSQN205I COUNT= 2, RETURN=00000000, REASON=00000004
CSQM137I +CSQ1 CSQMTCHI STOP CHINIT COMMAND ACCEPTED
CSQN205I COUNT= 2, RETURN=00000000, REASON=00000000
CSQ9022I +CSQ1 CSQXCRPS ' STOP CHINIT' NORMAL COMPLETION
(2)
CSQU057I CSQUCMDS 3 commands read
CSQU058I CSQUCMDS 3 commands issued and responses received, 0 failed
CSQU143I CSQUTIL 1 COMMAND statements attempted
CSQU144I CSQUTIL 1 COMMAND statements executed successfully
CSQU148I CSQUTIL Utility completed, return code=0
(3)

```

Obrázek 95. Příklad výstupu z CSQ4IVPX

Testování pro jazyky C, C + +, COBOL, PL/I a CICS

Můžete testovat jazyky C, C + +, COBOL, PL/I nebo CICS pomocí ukázkových aplikací dodaných s produktem IBM MQ.

IVP (CSQ4IVP1) je dodáván jako zaváděcí modul a poskytuje ukázky jako zdrojové moduly. Tyto zdrojové moduly můžete použít k testování různých prostředí programovacích jazyků.

Další informace o ukázkových aplikacích najdete v tématu [Ukázkové programy pro produkt IBM MQ for z/OS](#).

Nastavení komunikace s ostatními správci front

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS, které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

Chcete-li definovat požadavky na distribuované fronty, je třeba definovat následující položky:

- Definovat procedury inicializátoru kanálu a datové sady
- Definice definic kanálů
- Definování front a dalších objektů
- Definovat zabezpečení přístupu

Chcete-li povolit distribuované ukládání do fronty, je třeba provést následující tři úlohy:

- Upravte prostředek distribuovaného systému front a definujte vyžadované objekty produktu IBM MQ podle popisu v části Definování systémových objektů a “Příprava na přizpůsobení správců front produktu IBM MQ for z/OS” na stránce 523.
- Definujte zabezpečení přístupu, jak je popsáno v tématu Aspekty zabezpečení pro inicializátor kanálu na serveru z/OS.
- Nastavte komunikaci tak, jak je popsáno v tématu “Nastavení komunikace pro z/OS” na stránce 610.

Používáte-li skupiny sdílení front, prostudujte si téma Distribuované řazení do front a skupiny sdílení front.

Další informace o použití distribuovaných front s produktem IBM MQ for z/OS naleznete v následujících oddílech.

Operátorské zprávy

Protože iniciátor kanálu používá určitý počet asynchronně pracujících dispečerů, může dojít k tomu, že zprávy operátora se mohou vyskytnout v protokolu mimo chronologickou posloupnost.

Příkazy pro příkazy kanálu

Příkazy pro práci s kanály obvykle zahrnují dvě fáze. Pokud byla zkontrolována syntaxe příkazu a ověřena existence kanálu, odešle se požadavek na inicializátor kanálu. Zpráva CSQM134I nebo CSQM137I se odešle na vydavatele příkazu, aby označoval dokončení první fáze. Když iniciátor kanálu zpracoval příkaz, další zprávy označující její úspěch nebo jiné zprávy jsou odeslány vydavateli příkazu spolu se zprávou CSQ9022I nebo CSQ9023I. Jakékoli vygenerované chybové zprávy by se také mohly poslat na konzolu z/OS.

Všechny příkazy klastru kromě DISPLAY CLUSQMGR však pracují asynchronně. Příkazy, které mění atributy objektu, aktualizují objekt a odešlou požadavek na inicializátor kanálu. Příkazy pro práci s klastry se kontrolují na syntaxi a odešle se požadavek na iniciátor kanálu. V obou případech se odešle zpráva CSQM130I vydavateli příkazů označující, že požadavek byl odeslán. Tato zpráva je následována zprávou CSQ9022I, která označuje, že příkaz byl úspěšně dokončen v požadavku, který byl odeslán. Neoznačuje to, že požadavek klastru byl úspěšně dokončen. Požadavky odesílané na inicializátor kanálu jsou zpracovány asynchronně spolu s požadavky klastru přijatými od ostatních členů klastru. V některých případech musí být tyto požadavky odeslány na celý klaster, aby bylo možné určit, zda jsou úspěšné nebo ne. Jakékoli chyby jsou hlášeny na z/OS v systému, kde je spuštěn inicializátor kanálu. Neodesílají se vydavateli příkazů.

Nedoručená-fronta zpráv

Obslužná rutina nedoručенých zpráv je poskytována s produktem IBM MQ for z/OS. Další informace naleznete v tématu Obslužný program obslužné rutiny fronty nedoručенých zpráv (CSQUDLQH).

Fronty se používají

MCAs pro přijímací kanály může udržet cílové fronty otevřené i v případě, že zprávy nejsou přenášeny. Toto chování vede k tomu, že se fronty, které se objevují, používají 'v použití'.

Změny zabezpečení

Změníte-li bezpečnostní přístup pro ID uživatele, změna se nemusí projevit okamžitě. (Další informace naleznete v části Aspekty zabezpečení pro iniciátor kanálu v produktu z/OS, Profily pro zabezpečení fronty “Úloha 11: Implementovat ovládací prvky zabezpečení ESM” na stránce 543.)

Komunikace byla zastavena-TCP

Je-li protokol TCP z nějakého důvodu zastaven a poté restartován, bude zastaven modul listener TCP produktu IBM MQ for z/OS na portu TCP.

Automatický kanál-znovu navázat spojení umožňuje inicializátoru kanálu zjistit, že TCP/IP není k dispozici a při návratu TCP/IP automaticky restartovat modul listener TCP/IP. Tento automatický restart zmírňuje potřebu obsluhy problému s TCP/IP a ruční restart modulu listener. Když je modul listener mimo činnost, může být iniciátor kanálu také použit k pokusu modulu listener znovu v intervalu uvedeném v LSTRTMR. Tyto pokusy mohou pokračovat do doby, než se TCP/IP vrátí a modul listener se úspěšně restartuje automaticky. Informace o LSTRTMR viz [ALTER QMGR](#) a [Distributed queuing messages \(CSQX ...\)](#).

Zastavená komunikace- LU6.2

Dojde-li k zastavení APPC, zastaví se také modul listener. Opět platí, že v tomto případě se modul listener automaticky pokusí znovu spustit v intervalu LSTRTMR tak, že při restartu APPC se modul listener může restartovat také.

Pokud se Db2 nezdaří, sdílené kanály, které jsou již spuštěny, budou pokračovat, ale všechny nové požadavky na spuštění kanálu selžou. Když je Db2 obnoveno, nové požadavky jsou schopny dokončit.

z/OS Automatická správa restartu (ARM)

Automatic restart management (ARM) je funkce zotavení produktu z/OS , která může zlepšit dostupnost specifických dávkových úloh nebo spuštěných úloh (například subsystémů). Může tedy vést k rychlejšímu obnovení produktivní práce.

Chcete-li používat funkci ARM, je třeba nastavit správce front a iniciátory kanálu konkrétním způsobem, aby se restartovali automaticky. Další informace naleznete v tématu [Použití správce automatického restartu z/OS \(ARM\)](#).

Související pojmy

[“Konfigurace distribuovaných front” na stránce 124](#)

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

[“přízpůsobení IBM MQ for z/OS” na stránce 528](#)

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ .

[“Monitorování a řízení kanálů v systému z/OS” na stránce 594](#)

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front.

[“Nastavení komunikace pro z/OS” na stránce 610](#)

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nutné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak definovat připojení.

[“Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front” na stránce 614](#)

Pokyny v této sekci použijte ke konfiguraci distribuovaných front se skupinami sdílení front v systému IBM MQ for z/OS.

[“Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front” na stránce 618](#)

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení zadané v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby připojení bylo definováno a k dispozici.

Definování objektů IBM MQ

Použijte jednu z metod vstupu příkazu IBM MQ k definování objektů IBM MQ . Další podrobnosti o definování těchto objektů naleznete v informacích v tomto tématu.

Informace o definování objektů naleznete v příručce [“Monitorování a řízení kanálů v systému z/OS” na stránce 594](#) .

Přenosové fronty a spouštěcí kanály

Definujte následující:

- Lokální fronta s využitím XMITQ pro každý odesílající kanál zpráv.
- Definice vzdálených front.

Objekt vzdálené fronty má tři různé použití, v závislosti na způsobu, jakým je zadán název a obsah:


- Definice vzdálené fronty
- Definice aliasu správce front
- Definice alias fronty pro odpověď

Tyto tři způsoby jsou zobrazeny v části [Tři způsoby použití objektu definice vzdálené fronty](#).

Použijte pole TRIGDATA v přenosové frontě pro spuštění uvedeného kanálu. Příklad:

```
DEFINE QLOCAL(MYXMITQ) USAGE(XMITQ) TRIGGER +  
INITQ(SYSTEM.CHANNEL.INITQ) TRIGDATA(MYCHANNEL)  
DEFINE CHL(MYCHANNEL) CHLTYPE(SDR) TRPTYPE(TCP) +  
XMITQ(MYXMITQ) CONNAME('9.20.9.30(1555)')
```

Dodaný vzorek CSQ4INXD uvádí další příklady nezbytných definic.

 Ztráta konektivity ke struktuře prostředku mezipaměti klastru, kde je definována fronta synchronizace pro sdílené kanály nebo podobné problémy, může dočasně zabránit spuštění kanálu. Pokud při řešení problému používáte typ spouštěče FIRST a kanál se při spuštění nespustí, je třeba spustit kanál ručně. Chcete-li automaticky spustit spuštěné kanály po vyřešení problému, zvažte nastavení atributu TRIGINT správce front na jinou hodnotu než výchozí. Nastavení atributu TRIGINT na jinou hodnotu než výchozí nastavení způsobí, že inicializátor kanálu bude periodicky spouštět kanál, zatímco v přenosové frontě jsou zprávy.

Fronta synchronizace

DQM vyžaduje frontu pro použití s pořadovými čísly a identifikátory logických jednotek práce (LUWID). Musíte se ujistit, že je fronta k dispozici s názvem SYSTEM.CHANNEL.SYNCQ (viz [Plánování v systému z/OS](#)). Tato fronta musí být dostupná, jinak nelze spustit inicializátor kanálu.

Ujistěte se, že jste definovali tuto frontu pomocí INDXTYPE (MSGID). Tento atribut zlepšuje rychlost, ke které je možné přistupovat.

Fronty příkazů kanálu

Je třeba zajistit, aby pro systém existovala fronta příkazů kanálu s názvem SYSTEM.CHANNEL.INITQ.

Pokud inicializátor kanálu zjistí problém s parametrem SYSTEM.CHANNEL.INITQ nebude moci normálně pokračovat, dokud nebude problém odstraněn. Problém může být jeden z následujících:

- Fronta je plná
- Fronta není povolena pro vložení
- Sada stránek, na které je fronta zapnuta, je plná.
- Inicializátor kanálu nemá správné oprávnění zabezpečení pro frontu.

Pokud se definice fronty změní na GET (DISABLED), zatímco inicializátor kanálu běží, iniciátor není schopen získat zprávy z fronty a ukončuje se.

Spuštění inicializátoru kanálu

Spouštěcí impuls je implementován pomocí inicializátoru kanálu. V systému IBM MQ for z/OS je iniciátor spuštěn s příkazem MQSC START CHINIT.

Zastavení inicializátoru kanálu

Inicializátor kanálu se zastaví automaticky při zastavení správce front. Potřebujete-li zastavit iniciátor kanálu, ale ne správce front, můžete použít příkaz MQSC STOP CHINIT.

Monitorování a řízení kanálů v systému z/OS

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front.

Každý správce front produktu z/OS má program DQM (*inicializátor kanálu*). pro řízení propojení se vzdálenými správci front pomocí nativních zařízení produktu z/OS.

Implementace těchto panelů a příkazů v systému z/OS je integrována do operací a řídicích panelů a příkazů MQSC. V uspořádání těchto dvou sad panelů a příkazů se neodlišují žádné rozdíly.

Příkazy lze zadávat také pomocí příkazů PCF (Programmable Command Format). Informace o použití těchto příkazů najdete v tématu [Automatizace administrativních úloh](#).

Informace v této sekci se používají ve všech případech, kdy se používá inicializátor kanálu pro distribuované řazení do fronty. Používá se k tomu, zda používáte skupiny sdílení front nebo řazení do front v rámci skupiny.

Řídicí funkce kanálu DQM

Přehled modelu správy distribuovaných front viz [“Odeslání a příjem zprávy”](#) na stránce 145.

Řídicí funkce kanálu se skládá z panelů, příkazů a programů, dvou synchronizačních front, front příkazů kanálů a definic kanálů. Toto téma je stručným popisem komponent funkce řízení kanálů.

- Definice kanálů jsou uchovávány jako objekty na stránce nastavené jako nula nebo v Db2, stejně jako další objekty IBM MQ v z/OS.
- Použijte operace a řídicí panely, příkazy MQSC nebo příkazy PCF pro:
 - Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálu
 - Spustit a zastavit iniciátory kanálu a moduly listener
 - Kanály pro spuštění, zastavení a testování spojení, resetování pořadových čísel kanálů a řešení sporných zpráv, pokud nelze znovu zavést odkazy
 - Zobrazení informací o stavu kanálů
 - Zobrazit informace o aplikaci DQM

Konkrétně můžete použít vstupní datovou sadu inicializace CSQINPX pro zadání příkazů MQSC. Tato sada může být zpracována pokaždé, když spustíte inicializátor kanálu. Další informace viz téma [Inicializační příkazy](#).

- Existují dvě fronty (SYSTEM.CHANNEL.SYNCQ a SYSTEM.QSG.CHANNEL.SYNCQ) používaný pro účely opětného synchronizace kanálu. Definujte tyto fronty s INDEXTYPE (MSGID) z důvodu výkonu.
- Fronta příkazů kanálu (SYSTEM.CHANNEL.INITQ) se používá k ukládání příkazů pro iniciátory kanálu, kanály a moduly listener.
- Řídicí program kanálu pracuje ve svém vlastním adresním prostoru, odděleném od správce front a skládá se z iniciátoru kanálu, modulů listener, agentů MCA, monitoru spouštěčů a obslužné rutiny příkazů.
- Informace o skupinách sdílení front a sdílených kanálech naleznete v tématu [Sdílené fronty a skupiny sdílení front](#).
- Pro řazení do front v rámci skupiny naleznete informace v tématu [Řazení do front v rámci skupiny](#)

Správa kanálů v systému z/OS

Pomocí odkazů v následující tabulce naleznete informace o správě kanálů, inicializátorů kanálů a modulů listener:

<i>Tabulka 47. Úlohy kanálu</i>	
Úloha, která má být provedena	Příkaz MQSC
<u>Definovat kanál</u>	<u>Definovat kanál</u>
<u>Změna definice kanálu</u>	<u>ALTER CHANNEL</u>
<u>Zobrazení definice kanálu</u>	<u>DISPLAY CHANNEL</u>
<u>Odstranit definici kanálu</u>	<u>Odstranit kanál</u>
<u>Spustit inicializátor kanálu</u>	<u>START CHINIT</u>
<u>Zastavit inicializátor kanálu</u>	<u>STOP CHINIT</u>
<u>Zobrazit informace o inicializátoru kanálu</u>	<u>DISPLAY CHINIT</u>
<u>Spuštění modulu listener kanálu</u>	<u>Spustit listener</u>
<u>Zastavení modulu listener kanálu</u>	<u>Ukončit listener</u>
<u>Spuštění kanálu</u>	<u>Spustit kanál</u>
<u>Testovat kanál</u>	<u>Odeslat signál Ping pro kanál</u>
<u>Resetovat pořadová čísla zpráv pro kanál</u>	<u>Resetovat kanál</u>
<u>Vyřešit neověřené zprávy na kanálu</u>	<u>Vyřešit kanál</u>
<u>Zastavení kanálu</u>	<u>Ukončit kanál</u>
<u>Zobrazení stavu kanálu</u>	<u>ZOBRAZIT STAV CHSTATUS</u>
<u>Zobrazit kanály klastru</u>	<u>ZOBRAZIT CLUSQMGR</u>

Související pojmy

“Použití panelů a příkazů” na stránce 595

Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo ovládací panely a ovládací panely.

“Konfigurace distribuovaných front” na stránce 124

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

“Nastavení komunikace s ostatními správci front” na stránce 590

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS , které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

“přizpůsobení IBM MQ for z/OS” na stránce 528

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ .

“Nastavení komunikace pro z/OS” na stránce 610

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nutné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak definovat připojení.

“Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front” na stránce 614

Pokyny v této sekci použijte ke konfiguraci distribuovaných front se skupinami sdílení front v systému IBM MQ for z/OS.

“Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front” na stránce 618

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení zadané v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby připojení bylo definováno a k dispozici.

Použití panelů a příkazů

Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo ovládací panely a ovládací panely.

Informace o syntaxi příkazů MQSC najdete v tématu [Příkazy skriptu \(MQSC\)](#). Informace o příkazech PCF naleznete v části [Úvod do formátu Programovatelných příkazů](#).

Použití počátečního panelu

Úvod k vyvolání operací a řídicích panelů pomocí funkčních kláves a získání nápovědy najdete v tématu [Administrace produktu IBM MQ for z/OS](#).

Poznámka: Chcete-li používat operace a ovládací panely, musíte mít správnou autorizaci zabezpečení. Další informace naleznete v tématu [Administrace IBM MQ for z/OS](#) a dílčích témat. [Obrázek 96 na stránce 596](#) zobrazuje panel, který se zobrazí, když spustíte relaci panelu. Text poté, co panel vysvětluje akce, které provádíte na tomto panelu.

```
IBM MQ for z/OS - Main Menu

Complete fields. Then press Enter.

Action . . . . . 1 0. List with filter 4. Manage
1. List or Display 5. Perform
2. Define like 6. Start
3. Alter 7. Stop
8. Command
Object type . . . . . CHANNEL +
Name . . . . . *
Disposition . . . . . A Q=Qmgr, C=Copy, P=Private, G=Group,
S=Shared, A=All

Connect name . . . . . MQ25 - local queue manager or group
Target queue manager . . . MQ25
- connected or remote queue manager for command input
Action queue manager . . . MQ25 - command scope in group
Response wait time . . . . 10 5 - 999 seconds

(C) Copyright IBM Corporation 1993, 2023. All rights reserved.

Command ==>
F1=Help F2=Split F3=Exit F4=Prompt F9=SwapNext F10=Messages
F12=Cancel
```

Obrázek 96. Původní panel operací a ovládacích prvků

Na tomto panelu můžete:

- Vyberte akci, kterou chcete provést, zadáním odpovídajícího čísla do pole **Akce** .
- Uved'te typ objektu, se kterým chcete pracovat. Stiskněte klávesu F4 , abyste získali seznam typů objektů, pokud si nejste jisti, co jsou.
- Zobrazí seznam objektů zadaného typu. Zadejte hvězdičku (*) do pole **Název** a stisknutím klávesy Enter zobrazíte seznam objektů (zadaných typů), které již byly definovány v tomto subsystému. Pak můžete vybrat jeden nebo více objektů, se kterými chcete pracovat v posloupnosti. [Obrázek 97 na stránce 597](#) zobrazuje seznam kanálů vytvořených tímto způsobem.
- Do pole **Odebrání** zadejte dispozice v rámci skupiny sdílení front objektů, se kterými chcete pracovat. Dispozice určuje, kde je objekt uchován a jak se objekt chová.
- Vyberte lokálního správce front nebo skupinu sdílení front, ke které se chcete připojit, do pole **Název připojení** . Pokud chcete, aby příkazy byly vydány na vzdáleném správci front, vyberte buď pole **Cílový správce front** , nebo pole **Správce front akcí** , které závisí na tom, zda vzdálený správce front není nebo je členem skupiny sdílení front. Není-li vzdálený správce front členem žádné skupiny sdílení front, vyberte pole **Cílový správce front** . Je-li vzdálený správce front členem skupiny sdílení front, vyberte pole **Správce front akcí** .
- Zvolte čekací dobu na odpovědi, které mají být přijaty, do pole **Doba čekání na odpověď** .

List Channels - MQ25 Row 1 of 8

Type action codes, then press Enter. Press F11 to display connection status.
1=Display 2=Define like 3=Alter 4=Manage 5=Perform
6=Start 7=Stop

```
Name          Type      Disposition  Status
<> *          CHANNEL  ALL          MQ25
- SYSTEM.DEF.CLNTCONN CLNTCONN  QMGR  MQ25
- SYSTEM.DEF.CLUSRCVR CLUSRCVR  QMGR  MQ25 INACTIVE
- SYSTEM.DEF.CLUSSDR  CLUSSDR   QMGR  MQ25 INACTIVE
- SYSTEM.DEF.RECEIVER RECEIVER   QMGR  MQ25 INACTIVE
- SYSTEM.DEF.REQUESTER REQUESTER QMGR  MQ25 INACTIVE
- SYSTEM.DEF.SENDER   SENDER    QMGR  MQ25 INACTIVE
- SYSTEM.DEF.SERVER   SERVER     QMGR  MQ25 INACTIVE
- SYSTEM.DEF.SVRCONN  SVRCONN   QMGR  MQ25 INACTIVE
***** End of list *****
```

Command ==>
F1=Help F2=Split F3=Exit F4=Filter F5=Refresh F7=Bkwd
F8=Fwd F9=SwapNext F10=Messages F11=Status F12=Cancel

Obrázek 97. Výpis kanálů

Definování kanálu v systému z/OS

V systému z/OS můžete definovat kanál pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li definovat kanál pomocí příkazů MQSC, použijte [DEFINE CHANNEL](#).

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	2 (Definovat jako)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	
Dispozice	Umístění nového objektu.

Zobrazí se některé panely s informacemi o názvu a atributech, které chcete definovat pro kanál, který definujete. Inicializují se s výchozími hodnotami atributů. Před stisknutím klávesy Enter změňte všechny požadované hodnoty.

Poznámka: Pokud jste do pole **object type** zadali parametr CHANNEL, zobrazí se nejprve panel Vyberte platný typ kanálu.

Chcete-li definovat kanál se stejnými atributy jako existující kanál, zadejte název kanálu, který chcete zkopírovat, do pole **Name** na počátečním panelu. Panely jsou inicializovány s atributy existujícího objektu.

Další informace o atributech kanálů naleznete v tématu [Atributy kanálu](#)

Poznámka:

1. Pojmenujte všechny kanály v síti jedinečně. Jak je zobrazeno v [Síťový diagram zobrazující všechny kanály](#), včetně názvů zdrojového a cílového správce front v názvu kanálu je dobrý způsob, jak toto pojmenování provést.

Poté, co jste definovali svůj kanál, je třeba kanál zabezpečit, viz [“Zabezpečení kanálu” na stránce 599](#)

Změna definice kanálu

Definici kanálu můžete změnit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li změnit definici kanálu pomocí příkazů MQSC, použijte příkaz ALTER CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	3 (Změnit)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.ALTER
Dispozice	Umístění uloženého objektu.

Zobrazí se některé panely obsahující informace o aktuálních atributech kanálu. Změňte všechna nechráněná pole, která mají být přepsáním nové hodnoty, a poté stiskněte klávesu Enter, abyste změnili definici kanálu.

Další informace o atributech kanálů naleznete v tématu [Atributy kanálu](#).

Zobrazení definice kanálu

Definici kanálu můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit definici kanálu pomocí příkazů MQSC, použijte DISPLAY CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	1 (Seznam nebo zobrazení)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.DISPLAY
Dispozice	Umístění objektu.

Zobrazí se některé panely se zobrazením informací o aktuálních atributech kanálu.

Další informace o atributech kanálů naleznete v tématu [Atributy kanálu](#).

Odstranění definice kanálu

Definici kanálu můžete odstranit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li odstranit definici kanálu pomocí příkazů MQSC, použijte příkaz DELETE CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	4 (Spravovat)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.DELETE
Dispozice	Umístění objektu.

Zobrazí se vám jiný panel. Na tomto panelu vyberte typ funkce 1.

Stisknutím klávesy Enter odstraníte definici kanálu; budete požádáni o potvrzení, že chcete definici kanálu odstranit opětovným stisknutím klávesy Enter.

Poznámka: Inicializátor kanálu musí být spuštěn před odstraněním definice kanálu (s výjimkou kanálů připojení klienta).

Zobrazení informací o inicializátoru kanálu

Informace o inicializátoru kanálu můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit informace o inicializátoru kanálu pomocí příkazů MQSC, použijte příkaz DISPLAY CHINIT.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	1 (Zobrazit)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se vám jiný panel. Na tomto panelu vyberte typ funkce 1.

Poznámka:

1. Zobrazení distribuovaných informací o frontách může nějakou dobu trvat, pokud máte mnoho kanálů.
2. Inicializátor kanálu musí být spuštěn, než budete moci zobrazit informace o distribuovaných frontách.

Zabezpečení kanálu

Kanál můžete zabezpečit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zabezpečit kanál pomocí příkazů MQSC, použijte SET CHLAUTH.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	8

Zobrazí se editor, v němž můžete zadat příkaz MQSC, v tomto případě příkaz CHLAUTH, viz [Obrázek 98 na stránce 599](#). Po dokončení zápisu do příkazu je třeba použít znaménko plus (+). Zadejte příkaz PF3, chcete-li ukončit práci editoru a zadejte příkaz na příkazový server.

```
***** Top of Data *****
000001 SET CHLAUTH(SYSTEM.DEF.SVRCONN) +
000002 TYPE(SSLPEERMAP) +
000003 SSLPEER('CN="John Smith"') +
000004 MCAUSER('PUBLIC')
***** Bottom of Data *****

Command ==>                               Scroll ==> PAGE
F1=Help   F3=Exit   F4=LineEdit F12=Cancel
```

Obrázek 98. Zadání příkazů

Výstup příkazu se poté zobrazí, viz [Obrázek 99 na stránce 600](#)

```

***** ***** Top of Data *****
000001 CSQU000I CSQUTIL IBM MQ for z/OS V7.1.0
000002 CSQU001I CSQUTIL Queue Manager Utility - 2011-04-20 14:42:58
000003 COMMAND TGTQMGR(MQ23) RESPTIME(30)
000004 CSQU127I Executing COMMAND using input from CSQUCMD data set
000005 CSQU120I Connecting to MQ23
000006 CSQU121I Connected to queue manager MQ23
000007 CSQU055I Target queue manager is MQ23
000008 SET CHLAUTH(SYSTEM.DEF.SVRCONN) +
000009 TYPE(SSLPEERMAP) +
000010 SSLPEER('CN="John Smith"') +
000011 MCAUSER('PUBLIC')
000012 CSQN205I COUNT= 2, RETURN=00000000, REASON=00000000
000013 CSQ9022I !MQ23 CSQMCA ' SET CHLAUTH' NORMAL COMPLETION
000014 CSQU057I 1 commands read
000015 CSQU058I 1 commands issued and responses received, 0 failed
000016 CSQU143I 1 COMMAND statements attempted
000017 CSQU144I 1 COMMAND statements executed successfully
000018 CSQU148I CSQUTIL Utility completed, return code=0
Command ==> Scroll ==> PAGE
F1=Help F3=Exit F5=Rfind F6=Rchange F9=SwapNext F12=Cancel

```

Obrázek 99. Výstup příkazu

Spuštění inicializátoru kanálu

Inicializátor kanálu můžete spustit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li spustit inicializátor kanálu s použitím příkazů MQSC, použijte příkaz START CHINIT.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	6 (Začátek)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Spuštění systémových funkcí. Text na následujícím panelu vysvětluje, jaká akce se má provést:

```

Start a System Function

Select function type, complete fields, then press Enter to start system
function.

Function type . . . . . _ 1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
JCL substitution . . . . . -----
-----

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP
LU name (LU6.2) . . . . . -----
Port number (TCP/IP) . . . 1414
IP address (TCP/IP) . . . . . -----

Command ==> -----
F1=Help F2=Split F3=Exit F9=SwapNext F10=Messages F12=Cancel

```

Obrázek 100. Spuštění systémové funkce

Vyberte funkci typu 1 (inicializátor kanálu) a stiskněte klávesu Enter.

Zastavení inicializátoru kanálu

Inicializátor kanálu můžete zastavit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zastavit iniciátor kanálu pomocí příkazů MQSC, použijte příkaz STOP CHINIT.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	7 (Zastavit)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Zastavení systémových funkcí. Text následující po panelu vysvětluje, jak použít tento panel:

```
Stop a System Function

Select function type, complete fields, then press Enter to stop system
function.

Function type . . . . . _ 1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
Restart shared channels Y Y=Yes, N=No

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP

Port number (TCP/IP) . . . -----
IP address (TCP/IP) . . . -----

Command ==> _____
F1=Help F2=Split F3=Exit F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 101. Zastavení řízení funkce

Vyberte funkci typu 1 (inicializátor kanálu) a stiskněte klávesu Enter.

Inicializátor kanálu čeká na zastavení všech spuštěných kanálů v klidovém režimu, než se zastaví.

Poznámka: Jsou-li některé kanály přijímači nebo žadatelovými kanály, které jsou spuštěny, ale nejsou aktivní, požadavek na zastavení vydaný na přijímač nebo iniciátor kanálu odesílatele způsobí okamžité zastavení.

Pokud však zprávy procházejí, inicializátor kanálu čeká na dokončení aktuální dávky zpráv, než se zastaví.

Spuštění modulu listener kanálu

Přijímač kanálů můžete spustit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li spustit modul listener kanálu pomocí příkazů MQSC, použijte příkaz START LISTENER.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	6 (Začátek)

Pole	Hodnota
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Start a System Function (viz [Obrázek 100](#) na stránce 600).

Vyberte typ funkce 2 (modul listener kanálu). Vyberte volbu Příchozí odebrání. Vyberte typ přenosu. Je-li typ transportu L, vyberte název LU. Je-li typ transportu T, vyberte číslo portu a (volitelně) IP adresu. Stiskněte klávesu Enter.

Poznámka: Pro modul listener protokolu TCP/IP můžete spustit více kombinací portu a adresy IP.

Zastavení modulu listener kanálu

Příjímač kanálů můžete zastavit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zastavit modul listener kanálu pomocí příkazů MQSC, použijte příkaz STOP LISTENER.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	7 (Zastavit)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Zastavit systém System Function (viz [Obrázek 101](#) na stránce 601).

Vyberte typ funkce 2 (modul listener kanálu). Vyberte volbu Příchozí odebrání. Vyberte typ přenosu. Je-li typ transportu 'T', vyberte číslo portu a (volitelně) adresu IP. Stiskněte klávesu Enter.

Poznámka: V případě modulu listener protokolu TCP/IP můžete zastavit specifické kombinace portu a adresy IP nebo můžete zastavit všechny kombinace.

Spuštění kanálu

Kanál můžete spustit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li spustit kanál pomocí příkazů MQSC, použijte START CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	6 (Začátek)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Spustit kanál. Text na panelu vysvětluje, jak použít panel:

Start a Channel

Select disposition, then press Enter to start channel.

```
Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE
```

```
Disposition . . . . . P   P=Private on MQ25
S=Shared on MQ25
A=Shared on any queue manager
```

```
Command ==> -----
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 102. Spuštění kanálu

Vyberte dispozice instance kanálu a na tom, který správce front má být spuštěn.

Stisknutím klávesy Enter spustíte kanál.

Spuštění sdíleného kanálu

Chcete-li spustit sdílený kanál a ponechat jej na nominovaném inicializátoru kanálu, použijte dispozice = S (v příkazu START CHANNEL zadejte CHLDISP (FIXSHARED)).

V daném okamžiku může být spuštěna pouze jedna instance sdíleného kanálu. Pokusy o spuštění druhé instance kanálu selžou.

Spustíte-li kanál tímto způsobem, platí pro daný kanál následující pravidla:

- Kanál můžete zastavit z libovolného správce front ve skupině sdílení front. Můžete ji zastavit i v případě, že inicializátor kanálu, na kterém byla spuštěna, není spuštěna v době, kdy jste vydali požadavek na zastavení kanálu. Když je kanál zastaven, můžete jej restartovat uvedením dispozice = S (CHLDISP (FIXSHARED)) na stejném nebo jiném inicializátoru kanálu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Nachází-li se kanál ve stavu spuštění nebo opakování, můžete jej restartovat zadáním dispozice = S (CHLDISP (FIXSHARED)) na stejném nebo jiném inicializátoru kanálu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Kanál je způsobilý ke spuštění, když přejde do neaktivního stavu. Sdílené kanály, které spouštěč jsou spuštěny vždy, mají sdílenou dispozici (CHLDISP (SHARED)).
- Kanál je způsobilý ke spuštění s CHLDISP (FIXSHARED), na libovolném inicializátoru kanálu, když přejde do neaktivního stavu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Kanál není obnoven žádným jiným inicializačním kanálem ve skupině sdílení front, pokud byl inicializátor kanálu, ve kterém byla spuštěna, zastaven pomocí příkazu SHARED (RESTART), nebo při nestandardním ukončení inicializátoru kanálu. Kanál je obnoven pouze v případě, že inicializátor kanálu, na kterém byl spuštěn, bude znovu spuštěn. Tím se zastaví pokusy o zotavení kanálu, které byly předány ostatním inicializátoru kanálu ve skupině sdílení front, které by se přidaly do jejich pracovní zátěže.

Testování kanálu

Kanál můžete testovat pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li testovat kanál s použitím příkazů MQSC, použijte příkaz PING CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	5 (Provést)
Typ objektu	SENDER, SERVER, nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu kanálu.

Zobrazí se panel Provést funkci kanálu. Text na panelu vysvětluje, jak použít panel:

```
Perform a Channel Function
```

```
Select function type, complete fields, then press Enter.
```

```
Function type . . . . . _ 1. Reset 3. Resolve with commit  
2. Ping 4. Resolve with backout
```

```
Channel name . . . . . : CHANNEL.TO.USE  
Channel type . . . . . : SENDER  
Description . . . . . : Description of CHANNEL.TO.USE
```

```
Disposition . . . . . P P=Private on MQ25  
S=Shared on MQ25  
A=Shared on any queue manager
```

```
Sequence number for reset . . 1 1 - 999999999  
Data length for ping . . . . 16 16 - 32768
```

```
Command ==>
```

```
F1=Help F2=Split F3=Exit F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 103. Testování kanálu

Vyberte typ funkce 2 (příkaz ping).

Vyberte dispozice kanálu, pro který má být test proveden, a na kterém má být testován správce front.

Délka dat je na počátku nastavena na 16. Změňte jej, pokud chcete a stiskněte klávesu Enter.

Resetování pořadových čísel zpráv pro kanál

Pořadová čísla zpráv pro kanál můžete resetovat pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li resetovat pořadová čísla kanálů pomocí příkazů MQSC, použijte RESET CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	5 (Provést)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu kanálu.

Zobrazí se panel Provedení funkce kanálu (viz [Obrázek 103](#) na stránce 604).

Vyberte typ funkce 1 (reset).

Vyberte dispozice kanálu, pro který má být proveden reset, a na kterém má být proveden správce front.

Pole **Pořadové číslo** je na počátku nastaveno na hodnotu jedna. Změňte tuto hodnotu, pokud chcete, a stiskněte klávesu Enter.

Vyřešení nejistých zpráv na kanálu

Pochybné zprávy na kanálu můžete vyřešit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li vyřešit nejisté zprávy na kanálu pomocí příkazů MQSC, použijte RESOLVE CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	5 (Provést)
Typ objektu	SENDER, SERVER, nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Provedení funkce kanálu (viz [Obrázek 103 na stránce 604](#)).

Vyberte typ funkce 3 nebo 4 (interprete s potvrzením nebo vyřazováním). (Další informace viz [“Nejisté kanály”](#) na stránce 163 .)

Vyberte dispozice kanálu, pro který se má provést rozlišení a který správce front má být proveden. Stiskněte klávesu Enter.

Zastavení kanálu

Kanál můžete zastavit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zastavit kanál pomocí příkazů MQSC, použijte příkaz STOP CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	7 (Zastavit)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Zastavení kanálu. Text na panelu vysvětluje, jak použít panel:

Stop a Channel

Complete fields, then press Enter to stop channel.

```
Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE

Disposition . . . . . P   P=Private on MQ25
A=Shared on any queue manager

Stop mode . . . . . 1   1. Quiesce  2. Force
Stop status . . . . . 1   1. Stopped  2. Inactive

Queue manager . . . . . : _____
Connection name . . . . . : _____

Command ==> _____
F1=Help  F2=Split  F3=Exit  F9=SwapNext  F10=Messages  F12=Cancel
```

Obrázek 104. Zastavení kanálu

Vyberte dispozice kanálu, pro který má být zastaveno zastavení a na kterém má být zastaven správce front.

Zvolte režim zastavení, který požadujete:

Uvést do klidového stavu

Kanál se zastaví po dokončení aktuální zprávy a poté je dávka ukončena, i když nebyla dosažena hodnota velikosti dávky a zprávy již čekají na přenosovou frontu. Nejsou spuštěny žádné nové dávky. Tento režim je výchozí.

Vynutit

Kanál se zastaví okamžitě. Pokud probíhá zpracování dávky zpráv, může dojít k situaci 's nejistým stavem'.

Vyberte správce front a název připojení pro kanál, který chcete zastavit.

Vyberte stav, který požadujete:

Zastaveno

Kanál se automaticky nerestartuje a musí být restartován ručně. Tento režim je výchozí, není-li zadán žádný správce front nebo název připojení. Je-li uveden název, není to povoleno.

Neaktivní

Kanál se automaticky restartuje, je-li to nutné. Tento režim je výchozí, je-li zadán správce front nebo název připojení.

Stisknutím klávesy Enter zastavíte kanál.

Další informace viz [“Zastavení a uvedení kanálů do klidového stavu”](#) na stránce 161. Informace o restartování zastavených kanálů viz [“Restartování zastavených kanálů”](#) na stránce 162.

Poznámka: Je-li sdílený kanál ve stavu opakování a inicializátor kanálu, na kterém byl spuštěn, není spuštěn, je na správci front, ve kterém byl zadán příkaz, odeslán požadavek STOP pro kanál.

Zobrazení stavu kanálu

Stav kanálu můžete zobrazit pomocí příkazů MQSC, nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit stav kanálu nebo sady kanálů pomocí příkazů MQSC, použijte příkaz DISPLAY CHSTATUS.

Poznámka: Zobrazení informací o stavu kanálu může nějakou dobu trvat, máte-li mnoho kanálů.

Při použití operací a ovládacích panelů na panelu Seznam kanálů (viz téma [Obrázek 97](#) na stránce 597) je pro každý kanál zobrazen souhrn stavu kanálu následovně:

NEAKTIVNÍ	Nejsou aktivní žádná připojení
<i>stav</i>	Jedno připojení je aktivní
<i>nnn stav</i>	Více než jedno připojení je aktuální a všechna aktuální připojení mají stejný stav
<i>nnn CURRENT</i>	Více než jedno připojení je aktuální a aktuální připojení nemají všechny stejný stav.
Prázdný	IBM MQ nemůže určit, kolik připojení je aktivních (například, protože inicializátor kanálu není spuštěn)

Poznámka: U objektů kanálu s dispozicí GROUP není zobrazen žádný stav.

kde *nnn* je počet aktivních připojení a *stav* je jeden z následujících:

Inicializovat	INICIALIZACE
BIND	Vazba
SPUSTIT	SPOUŠTĚNÍ
RUN	RUNNING
ZASTAVIT	ZASTAVOVÁNÍ nebo ZASTAVENO
RETRY	Opakovaný pokus
REQST	Zpracování požadavků

Chcete-li zobrazit další informace o stavu kanálu, stiskněte klávesu Stav (F11) na kanálu seznamu nebo obrazovky nebo změňte panely kanálu a zobrazí se panel Seznam kanálů-Aktuální stav (viz [Obrázek 105](#) na stránce 607).

```
List Channels - Current Status - MQ25      Row 1 of 16
Type action codes, then press Enter. Press F11 to display saved status.
1=Display current status

Channel name      Connection name      State
Start time      Messages Last message time Type Disposition
<> *
CHANNEL ALL MQ25
- RMA0.CIRCUIT.ACL.F RMA1 STOP
- 2005-03-21 10.22.36 557735 2005-03-24 09.51.11 SENDER PRIVATE MQ25
- RMA0.CIRCUIT.ACL.N RMA1
- 2005-03-21 10.23.09 378675 2005-03-24 09.51.10 SENDER PRIVATE MQ25
- RMA0.CIRCUIT.CL.F RMA2
- 2005-03-24 01.12.51 45544 2005-03-24 09.51.08 SENDER PRIVATE MQ25
- RMA0.CIRCUIT.CL.N RMA2
- 2005-03-24 01.13.55 45560 2005-03-24 09.51.11 SENDER PRIVATE MQ25
- RMA1.CIRCUIT.CL.F RMA1
- 2005-03-21 10.24.12 360757 2005-03-24 09.51.11 RECEIVER PRIVATE MQ25
- RMA1.CIRCUIT.CL.N RMA1
- 2005-03-21 10.23.40 302870 2005-03-24 09.51.09 RECEIVER PRIVATE MQ25
***** End of list *****
Command ==>
F1=Help F2=Split F3=Exit F4=Filter F5=Refresh F7=Bkwd
F8=Fwd F9=SwapNext F10=Messages F11=Saved F12=Cancel
```

Obrázek 105. Výpis připojení kanálů

Hodnoty stavu jsou následující:

Inicializovat	INICIALIZACE
---------------	--------------

BIND	Vazba
SPUSTIT	SPOUŠTĚNÍ
RUN	RUNNING
ZASTAVIT	ZASTAVOVÁNÍ nebo ZASTAVENO
RETRY	Opakovaný pokus
REQST	Zpracování požadavků
POCHYBNÉ	ZASTAVENO a INDOUBT (YES)

Další informace viz [“Stavy kanálů”](#) na stránce 154.

Můžete stisknout klávesu F11 , abyste zobrazili podobný seznam připojení kanálů s uloženým stavem; stiskněte klávesu F11 , abyste se vrátili zpět na aktuální seznam. Uložený stav se neuplatní, dokud nebude na kanálu přenesena alespoň jedna dávka zpráv.

Použijte aktivační kód 1 nebo lomítko (/) pro výběr připojení a stiskněte klávesu Enter. Zobrazí se panely Zobrazit aktuální stav připojení kanálu.

Zobrazení kanálů klastru

Kanály klastru můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit všechny kanály klastru, které byly definovány (explicitně nebo s použitím automatické definice), použijte příkaz MQSC, DISPLAY CLUSQMGR.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	1 (Seznam nebo zobrazení)
Typ objektu	CLUSCHL
Název	*

Zobrazí se panel jako obrázek [Obrázek 106 na stránce 609](#), v němž informace pro každý kanál klastru zaujímají tři řádky a obsahují názvy jeho kanálů, klastrů a správců front. Pro odesílací kanály klastru se zobrazí celkový stav.


```

List Cluster-queue-manager Channels - MQ25      Row 1 of 9

Type action codes, then press Enter. Press F11 to display connection status.
1=Display 5=Perform 6=Start 7=Stop

Channel name      Connection name      State
Type      Cluster name      Suspended
Cluster queue manager name      Disposition
<> *
- TO.MQ90.T      HURSLEY.MACH90.COM(1590)
- CLUSRCVR      VJH01T      N
- MQ90      -      MQ25
- TO.MQ95.T      HURSLEY.MACH95.COM(1595)      RUN
- CLUSSDRA      VJH01T      N
- MQ95      -      MQ25
- TO.MQ96.T      HURSLEY.MACH96.COM(1596)      RUN
- CLUSSDRB      VJH01T      N
- MQ96      -      MQ25
***** End of list *****

Command ==>
F1=Help  F2=Split  F3=Exit  F4=Filter  F5=Refresh  F7=Bkwd
F8=Fwd  F9=SwapNext  F10=Messages  F11=Status  F12=Cancel

```

Obrázek 106. Zobrazení seznamu kanálů klastru

Chcete-li zobrazit úplné informace o jednom nebo více kanálech, zapište kód akce 1 proti jejich jménům a stiskněte klávesu Enter. Použijte kódy akce 5, 6 nebo 7 k provedení funkcí (jako např. ping, resolve a reset) a spuštění nebo zastavení kanálu klastru.

Chcete-li zobrazit další informace o stavu kanálu, stiskněte klávesu Stav (F11).

Příprava produktu IBM MQ for z/OS k použití funkce produktu zEnterprise Data Compression Express

Prostředek produktu zEnterprise Data Compression (zEDC) Express je k dispozici pro určité modely počítačů se systémem IBM Z, počínaje verzí IBM zEC12 GA2, s použitím minimální úrovně z/OS produktu z/OS 2.1.

Další informace viz [zEnterprise Data Compression \(zEDC\)](#).

Požadavky

Pro IBM z15 a později byla funkce produktu zEnterprise Data Compression (zEDC) Express přesunuta z volitelné funkce v zásuvce I/O PCIe na hardwarovém systému, aby byla na čipu jako integrovaný akcelerátor pro zEDC. S touto změnou se aktualizují předpoklady konfigurace a jsou závislé na vašem hardwarovém systému.

IBM z15 nebo vyšší

V závislosti na úrovni operačního systému z/OS použijte jednu z následujících oprav PTF:

- z/OS 2.5: UJ00639
- z/OS 2.4: UJ00636
- z/OS 2.3: UJ00635
- z/OS 2.2: UJ00638

Pro systémy z15 nebo pozdější neexistují žádné požadavky na hardware. Integrovaný akcelerátor pro řešení zEDC v těchto systémech poskytuje vestavěnou akceleraci dat, takže samostatný adaptér již není zapotřebí.

IBM zEC12 GA2 až IBM z14

Váš systém musí mít také tyto požadavky:

- Adaptér zEDC Express[®] instalovaný v zásuvkách I/O PCIe na hardwarovém systému.
- Schopnost softwaru zEDC (volitelná komponenta naiv-for) musí být povolena v členu knihovny parametrů IFAPRDxx.

Postup

IBM zEC12 GA2 až IBM z14

Ujistěte se, že ID uživatele iniciátoru kanálu má oprávnění READ pro FPZ.ACCELERATOR.COMPRESSION ve třídě FACILITY CLASS produktu RACF nebo ekvivalent v externím správci zabezpečení (ESM), který váš podnik používá.



Upozornění: Nepožaduje se pro IBM z15 nebo novější.

IBM zEnterprise zEC12 GA2 nebo novější

Konfigurujte kanál s parametrem COMPMSG (ZLIBFAST) na konci odesílání i příjmu. Po konfiguraci je komprese zlib použita ke kompresi a dekomprimaci zpráv procházejících přes kanál.

Komprese se provádí v zEDC, pokud velikost dat, která mají být komprimována, je nad minimální prahovou hodnotou. Prahová hodnota je závislá na použitém hardwaru produktu IBM z.

- IBM zEC12 GA2 až IBM z14 má minimální prahovou hodnotu 4KB
- IBM z15 nebo pozdější má minimální prahovou hodnotu 1KB

Pro zprávy pod prahovou hodnotou je komprese nebo inflace prováděna v softwaru.

Nastavení komunikace pro z/OS

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nutné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak definovat připojení.

DQM je prostředek vzdáleného řazení do fronty pro produkt IBM MQ. Poskytuje řídicí programy kanálu pro správce front, který tvoří rozhraní pro komunikační propojení. Tyto odkazy jsou kontrolovatelné systémovým operátorem. Definice kanálů, které jsou v držení distribuované správy front, používají tato připojení.

Vyberte si z jedné ze dvou forem komunikačního protokolu, které lze použít pro z/OS:

- [“Definování připojení TCP na systému z/OS”](#) na stránce 611
- [“Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS”](#) na stránce 613

Každá definice kanálu musí určovat pouze jeden protokol jako atribut přenosového protokolu (Typ transportu). Správce front může ke komunikaci použít více než jeden protokol.

Může se také stát, že bude užitečné se podívat na téma [Příklad konfigurace- IBM MQ for z/OS](#). Pokud používáte skupiny sdílení front, prohlédněte si téma [“Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front”](#) na stránce 618.

Související pojmy

[“Použití panelů a příkazů”](#) na stránce 595

Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo ovládací panely a ovládací panely.

[“Konfigurace distribuovaných front”](#) na stránce 124

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ, včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

[“Nastavení komunikace s ostatními správci front”](#) na stránce 590

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS, které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

[“přizpůsobení IBM MQ for z/OS” na stránce 528](#)

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ .

[“Monitorování a řízení kanálů v systému z/OS” na stránce 594](#)

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front.

[“Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front” na stránce 614](#)

Pokyny v této sekci použijte ke konfiguraci distribuovaných front se skupinami sdílení front v systému IBM MQ for z/OS.

[“Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front” na stránce 618](#)

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení zadané v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby připojení bylo definováno a k dispozici.

Definování připojení TCP na systému z/OS

Chcete-li definovat připojení TCP, je zde několik nastavení, které je třeba nakonfigurovat.

Název adresního prostoru TCP musí být zadán v datové sadě systémových parametrů protokolu TCP, *tcip*.TCPIP.DATA. V datové sadě musí být zahrnut příkaz "TCPIPJOBNAME *TCPIP_proc*".

Používáte-li bránu firewall, je třeba konfigurovat připojení produktu `allow` z inicializátoru kanálu k adresám v kanálech a ze vzdálených připojení do správce front.

Definice brány firewall obvykle konfiguruje odesílající adresu IP a port do cílové adresy IP a portu:

- Obraz produktu z/OS může mít více než jeden název hostitele a může být zapotřebí nakonfigurovat bránu firewall s více adresami hostitele jako zdrojovou adresou.

Chcete-li zobrazit tyto názvy a adresy, můžete použít příkaz `NETSTAT HOME`.

- Inicializátor kanálu může mít několik modulů listener na různých portech, takže je třeba tyto porty nakonfigurovat.
- Používáte-li sdílený port pro skupinu sdílení front, je třeba také nakonfigurovat sdílený port.

Adresní prostor inicializátoru kanálu musí mít oprávnění ke čtení datové sady. Následující techniky lze použít pro přístup k vašim `TCPIP.DATA` datové sady, v závislosti na tom, jaký produkt a rozhraní TCP/IP používáte:

- Proměnná prostředí, `RESOLVER_CONFIG`
- HFS soubor, `/etc/resolv.conf`
- `// SYSTCPD DD`, příkaz
- `// SYSTCPDD DD`, příkaz
- `jobname/userid.TCPIP.DATA`
- `SYS1.TCPPARMS(TCPDATA)`
- `zapname.TCPIP.DATA`

Musíte také být opatrní, abyste správně zadali kvalifikátor vyšší úrovně pro TCP/IP.

Potřebujete vhodně nakonfigurovaný server DNS (Domain Name System) schopný jak překlad adres IP, tak překlad adres IP na překlad názvů.

Poznámka: Některé změny v konfiguraci vyhodnocovacího modulu vyžadují recyklování aplikací, které jej používají, například IBM MQ.

Další informace jsou uvedeny v následujících tématech:

- [Základní systém TCP/IP](#)
- [Systémové služby produktů z/OS UNIX](#).

Každý kanál TCP při spuštění používá prostředky TCP; možná budete muset upravit následující parametry ve vašem `PROFILE.TCPIP` :

VELIKOST FONDU ABPOOLSIZE

Přidejte jeden z spuštěných kanálů TCP a jeden z nich.

CCBPOOLSIZE

Přidejte jeden každý spuštěný kanál TCP a jeden pro každý dispečer DQM, plus jeden.

VELIKOST DATABUFFERPOOLSIZ

Přidejte dva pro každý spuštěný kanál TCP plus jeden.

MAXFILEPROC

Řídí, kolik kanálů může každý dispečer v inicializátoru kanálu zpracovat.

Tento parametr je uveden ve členu BPXPRMxx SYSLPARMLIB. Ujistěte se, že jste zadali dostatečně velkou hodnotu pro vaše potřeby.

Inicializátor kanálu je ve výchozím nastavení schopen pouze vazby na adresy IP přidružené k zásobníku uvedenému v atributu správce front TCPNAME. Chcete-li povolit inicializátoru kanálu komunikovat s použitím dalších zásobníků TCP/IP na systému, změňte atribut správce front TCPSTACK na hodnotu MULTIPLE.

Související pojmy

“Odesílání: Konec” na stránce 612

Na odesílajícím konci připojení TCP/IP existuje několik nastavení, které je třeba nakonfigurovat.

“Příjem na TCP” na stránce 612

Na přijímajícím konci připojení TCP/IP je zde několik nastavení, které lze konfigurovat.

“Použití volby nevyřízených požadavků na modul listener TCP” na stránce 613

Při příjmu v protokolu TCP/IP je nastaven maximální počet neprovedených požadavků na připojení. Tyto nevyřízené požadavky mohou být považovány za *nevyřízené požadavky* požadavků čekajících na portu TCP/IP pro modul listener, aby přijal požadavek.

Odesílání: Konec

Na odesílajícím konci připojení TCP/IP existuje několik nastavení, které je třeba nakonfigurovat.

Pole názvu připojení (CONNNAME) v definici kanálu musí být nastaveno buď na název hostitele (například MVSHUR1), nebo na síťovou adresu TCP cíle. Síťová adresa TCP může být v tečkovém desítkovém tvaru IPv4 (například 127.0.0.1) nebo v hexadecimální formě IPv6 (například 2001:DB8:0:0:0:0:0:0). Je-li název připojení název hostitele, je požadován server názvů TCP pro převedení názvu hostitele na adresu hostitele TCP. (Tento požadavek je funkce protokolu TCP, nikoli IBM MQ.)

Na zahajovacím konci připojení (typy kanálů odesílatele, žadatele a serveru) je možné poskytnout volitelné číslo portu pro připojení, například:

Název připojení

192.0.2.0(1555)

V tomto případě se iniciující ukončení pokusí o připojení k přijímajícímu programu naslouchajícího na portu 1555.

Poznámka: Je-li zadáno volitelné číslo portu, použije se výchozí číslo portu 1414.

Inicializátor kanálu může použít libovolný zásobník TCP/IP, který je aktivní a dostupný. Inicializátor kanálu standardně sváže odchozí kanály s výchozí adresou IP pro zásobník TCP/IP, pojmenovaný v atributu správce front TCPNAME. Chcete-li se připojit přes jiný zásobník, musíte uvést buď název hostitele, nebo adresu IP zásobníku v atributu LOCLADDR kanálu.

Příjem na TCP

Na přijímajícím konci připojení TCP/IP je zde několik nastavení, které lze konfigurovat.

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu START LISTENER nebo pomocí operací a řídicích panelů.

Ve výchozím nastavení:

- Program TCP Listener používá port 1414 a naslouchá na všech adresách, které jsou dostupné pro zásobník TCP.

- Moduly listener protokolu TCP/IP se mohou vázat pouze na adresy přidružené k zásobníku TCP/IP jmenovanému v atributu správce front TCPNAME.

Chcete-li spustit listenery pro jiné adresy nebo všechny dostupné zásobníky TCP, nastavte atribut správce front TCPSTACK na 'MULTIPLE'.

Program modulu listener TCP můžete spustit tak, aby naslouchal pouze na určité adrese nebo názvu hostitele, zadáním IPADDR v příkazu START LISTENER. Další informace viz [Moduly listener](#).

Použití volby nevyřízených požadavků na modul listener TCP

Při příjmu v protokolu TCP/IP je nastaven maximální počet neprovedených požadavků na připojení. Tyto nevyřízené požadavky mohou být považovány za *nevyřízené požadavky* požadavků čekajících na portu TCP/IP pro modul listener, aby přijal požadavek.

Výchozí hodnota nahromadění modulu listener v systému z/OS je 255. Pokud jsou tyto hodnoty nahromadění nevyřízených požadavků, je připojení TCP/IP zamítnuto a kanál se nemůže spustit.

V případě kanálu MCA se výsledkem tohoto výsledku v kanálu stane stav ZOPAKOVAT a později se znovu pokusí o připojení.

V případě připojení klienta obdrží klient kód příčiny MQRQ_Q_MGR_NOT_AVAILABLE z objektu MQCONN a později se může připojení pokusit o zopakování připojení.

Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS

Chcete-li definovat připojení LU6.2, je třeba nakonfigurovat několik nastavení.

Nastavení APPC/MVS

Každá instance inicializátoru kanálu musí mít název jednotky LU, kterou má být nadefinován pro APPC/MVS, ve členu APPCPMxx SYS1.PARMLIB, jako v následujícím příkladu:

```
LUADD ACBNAME( luname ) NOSCHED TPDATA(CSQ.APPCTP)
```

luname je název logické jednotky, která má být použita. NOSCHED je povinný; TPDATA se nepoužije. Pro člen ASCHPMxx nebo pro datovou sadu profilu APPC/MVS TP nejsou nutná žádná doplnění.

Datová sada bočních informací musí být rozšířena, aby definovala připojení použitá aplikací DQM. Podrobné informace o tom, jak postupovat při použití obslužného programu ATBSDFMU, najdete v dodané ukázce CSQ4SIDE. Chcete-li získat podrobnosti o hodnotách TPNAME, prohlédněte si následující tabulku, kde získáte informace:

<i>Tabulka 48. Nastavení na lokálním systému z/OS pro vzdálenou platformu správce front</i>	
Vzdálená platforma	TPNAME
z/OS nebo MVS	Tentýž jako TPNAME v odpovídajících informacích o vzdáleném správci front.
IBM i	Stejně jako porovnávací hodnota v záznamu směrování v systému IBM i.
HP Integrity NonStop Server	Stejně jako název TPNAME uvedený v definici kanálu příjemce.
Systémy SYSTÉM UNIX a Linux	Tentýž jako TPNAME v odpovídajících informacích o vzdáleném správci front.
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nevolnitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.

Pokud máte na jednom počítači více než jednoho správce front, ujistěte se, že názvy TPnames v definicích kanálů jsou jedinečné.

Další informace o definicích modulů VTAM, které mohou být vyžadovány, naleznete v příručce *Multiplatform APPC Configuration Guide*.

V prostředí, ve kterém správce front komunikuje pomocí APPC se správcem front ve stejném nebo v jiném systému z/OS, zkontrolujte, zda definice VTAM pro komunikační LU určuje SECACPT (ALREADYV), nebo že existuje profil RACF APPCLU pro připojení mezi jednotkami LU, který uvádí CONVSEC (ALREADYV).

Příkaz z/OS VARY ACTIVE musí být před pokusem o spuštění příchozí nebo odchozí komunikace vydán proti jednotkám LU Base a modulu listener.



Upozornění: Kromě nastavení APPC je třeba zadat následující příkaz:

```
ALTER QMGR LUNAME(1uname)
```

a restartujte inicializátor kanálu.

Další informace viz [LUNAME](#).

Související pojmy

“Připojování k LU 6.2” na stránce 614

Chcete-li se připojit k LU 6.2, je třeba nakonfigurovat několik nastavení.

“Příjem na LU 6.2” na stránce 614

Pro přijetí na LU 6.2 existuje několik nastavení, které je třeba nakonfigurovat.

Připojování k LU 6.2

Chcete-li se připojit k LU 6.2, je třeba nakonfigurovat několik nastavení.

Pole názvu připojení (CONNNAME) v definici kanálu musí být nastaveno na symbolický název cíle, jak je uvedeno v datové sadě informací o připojení pro APPC/MVS.

Název jednotky LU, který má být použit (definovaný pro parametr APPC/MVS, jak je popsáno výše), musí být také zadán v parametrech inicializátoru kanálu. Musí být nastaven na stejnou logickou jednotku, která je používána pro příjem posluchače.

Inicializátor kanálu používá volbu APPC/MVS "SECURITY (SAME)", takže se jedná o ID uživatele adresního prostoru iniciátoru kanálu, který se používá pro odchozí přenosy, a je předložen příjemci.

Příjem na LU 6.2

Pro přijetí na LU 6.2 existuje několik nastavení, které je třeba nakonfigurovat.

Příjem MCA se spouští jako odezva na požadavek spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Program modulu listener je server APPC/MVS. Spustíte ji pomocí příkazu START LISTENER nebo pomocí operací a řídicích panelů. Je třeba určit název jednotky LU, který má být použit se symbolickým názvem místa určení definovaným v datové sadě informací o připojení. Identifikovaná lokální LU musí být stejná jako ta, která se používá pro odchozí přenosy, jak je nastaveno v parametrech inicializátoru kanálu.

Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front

Pokyny v této sekci použijte ke konfiguraci distribuovaných front se skupinami sdílení front v systému IBM MQ for z/OS.

Příklad konfigurace s použitím skupin sdílení front viz [Příklad konfigurace- IBM MQ for z/OS pomocí skupin sdílení front](#). Příklad plánování kanálu zpráv s použitím skupin sdílení front naleznete v tématu [Příklad plánování kanálů zpráv pro produkt z/OS s použitím skupin sdílení front](#).

Chcete-li povolit distribuované řazení do front se skupinami sdílení front, je třeba vytvořit a nakonfigurovat následující komponenty:

- [Moduly listener LU 6.2 a TCP/IP](#)
- [Přenosové fronty a spuštění](#)
- [Agenti kanálů zpráv](#)
- [Fronta synchronizace](#)

Poté, co jste vytvořili komponenty potřebné k nastavení komunikace, prohlédněte si téma [“Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front”](#) na stránce 618.

Informace o tom, jak monitorovat a řídit kanály při použití skupin sdílení front, viz [“Monitorování a řízení kanálů v systému z/OS”](#) na stránce 594.

Informace o koncepcích a výhodách a výhodách skupiny sdílení front naleznete v následujících oddílech.

Třída služeb

Sdílená fronta je typem lokální fronty, která nabízí jinou třídu služeb. Zprávy v rámci sdílené fronty jsou uloženy v prostředku CF (coupling facility), který jim umožňuje přístup ke všem správcům front ve skupině sdílení front. Zpráva ve sdílené frontě musí být zpráva o délce nejvýše 100 MB.

Generické rozhraní

Skupina sdílení front má generické rozhraní, které umožňuje, aby síť prohlížela skupinu jako jedinou entitu. Toto zobrazení je dosaženo pomocí jediné generické adresy, kterou lze použít pro připojení k libovolnému správci front v rámci skupiny.

Každý správce front ve skupině sdílení front naslouchá požadavkům příchozí relace na adrese, která je logicky spojena s generickou adresou. Další informace viz [“Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front”](#) na stránce 616.

Začátek vyrovnaného kanálu

Sdílenou přenosovou frontu může obsloužit odchozí kanál, který je spuštěn na libovolném inicializátoru kanálu ve skupině sdílení front. Spuštění kanálu s vyrovnáním zátěže určuje, kde je zacílen příkaz ke spuštění kanálu. Je zvolen vhodný inicializátor kanálu, který má přístup k nezbytným komunikačním subsystémům. Například kanál definovaný s TRPTYPE (LU6.2) nemůže být spuštěn na inicializátoru kanálu, který má pouze přístup k subsystému TCP/IP.

Volba inicializátoru kanálu závisí na zatížení kanálu a na hlavní místnosti iniciátoru kanálu. Zatížení kanálu je počet aktivních kanálů vyjádřený jako procentní podíl maximálního počtu povolených aktivních kanálů, jak je definováno v parametrech inicializátoru kanálu. Místnost je rozdíl mezi počtem aktivních kanálů a maximálním přípustným počtem kanálů.

Příchozí sdílené kanály mohou být vyrovnány do skupiny sdílení front použitím generické adresy, jak je popsáno v tématu [“Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front”](#) na stránce 616.

Obnova sdíleného kanálu

V následující tabulce jsou uvedeny typy selhání se sdílenými kanály a způsob zpracování jednotlivých typů.

Typ selhání:	Co se děje:
Selhání komunikačního subsystému inicializátoru kanálu	Kanály závislé na komunikačním subsystému vstupují do kanálu znovu a jsou restartovány u příslušného inicializátoru kanálu se skupinou sdílení front pomocí příkazu ke spuštění s vyrovnáním zátěže.
Selhání inicializátoru kanálu	Inicializátor kanálu selže, ale přidružený správce front zůstane aktivní. Správce front monitoruje selhání a zahajuje zpracování zotavení.
Selhání správce front	Dojde k selhání správce front (selhání přidruženého iniciátoru kanálu). Ostatní správci front v rámci skupiny sdílení front monitorují událost a zahájí partnerské zotavení.

Selhání sdíleného stavu	Informace o stavu kanálu jsou uloženy v produktu Db2, takže ztráta konektivity k produktu Db2 se stane selháním, pokud dojde ke změně stavu kanálu. Spuštěné kanály mohou provádět provoz bez přístupu k těmto prostředkům. Při neúspěšném přístupu k produktu Db2 se kanál znovu pokusí o opakování.
-------------------------	---

Zpracování zotavení sdíleného kanálu pro systém, který selhal, vyžaduje připojení k produktu Db2, které má být k dispozici v systému spravujícím obnovu k načtení stavu sdíleného kanálu.

Kanály klienta

Kanály připojení klienta mohou těžit z vysoké dostupnosti zpráv ve skupinách sdílení front, které jsou připojeny k generickému rozhraní místo toho, aby byly připojeny ke specifickému správci front. Další informace naleznete v tématu [Kanály připojení klienta](#).

Související pojmy

[“přizpůsobení IBM MQ for z/OS” na stránce 528](#)

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ.

[“Konfigurace distribuovaných front” na stránce 124](#)

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ, včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

[“Nastavení komunikace s ostatními správci front” na stránce 590](#)

Tento oddíl popisuje přípravy produktu IBM MQ for z/OS, které je třeba provést před zahájením práce s distribuovaným řazením do fronty.

[“Klastry a skupiny sdílení front” na stránce 618](#)

Sdílenou frontu můžete zpřístupnit pro klastr v jediné definici. Chcete-li tak učinit, zadejte při definování sdílené fronty název klastru.

[“Kanály a serializace” na stránce 618](#)

Během partnerské obnovy sdílené fronty zpráv kanálu zpráv, které zpracovávají zprávy ve sdílených frontách, serializuje jejich přístup k frontám.

Související informace

[Sdílené fronty a skupiny sdílení front](#)

[Použití front v rámci skupiny](#)

Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front

Skupině LU 6.2 a posluchači TCP/IP naslouchají na adrese, která je logicky připojena ke generické adrese.

V případě modulu listener LU 6.2 je uvedená skupina LUGROUP mapována na generický prostředek VTAM přidružený ke skupině sdílení front. Příklad nastavení této technologie viz [“Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS” na stránce 613](#).

V případě modulu listener protokolu TCP/IP může být uvedený port připojen k obecné adrese jedním z následujících způsobů:

- Pro front-endový směrovač, jako je například IBM Network Dispatcher, jsou příchozí požadavky na připojení přesměrovány ze směrovače na členy skupiny sdílení front.
- Pro distributor prostředí sysplex protokolu TCP/IP je každý modul listener, který běží a naslouchá na konkrétní adrese, která je nastavena jako distribuovaná DVIPA, přidělen poměrům příchozích požadavků. Příklad nastavení této technologie naleznete v tématu [Použití distributoru prostředí sysplex](#).

Přenosové fronty a spuštění pro skupiny sdílení front

Sdílená přenosová fronta se používá k ukládání zpráv před přesunutím ze skupiny sdílení front do cíle.

Jedná se o sdílenou frontu a je přístupná pro všechny správce front ve skupině sdílení front.

Spouštění

Spuštěná sdílená fronta může vygenerovat více než jednu zprávu spouštěče pro splněnou podmínku spouštěče. Pro každou lokální inicializační frontu definovanou ve správci front v rámci skupiny sdílení front přidružené ke spuštěné sdílené frontě je vygenerována jedna zpráva spouštěče.

Pro distribuované řazení do fronty obdrží každý iniciátor kanálu zprávu spouštěče pro splněnou podmínku spouštěče sdílené přenosové fronty. Ale pouze jeden iniciátor kanálu skutečně zpracovává spuštěný start a ostatní selžou bezpečně. Spuštěný kanál je poté spuštěn s vyrovnáním zátěže (viz [“Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front”](#) na stránce 614). který se spustí ke spuštění kanálu QSG . TO . QM2. Chcete-li vytvořit sdílenou přenosovou frontu, použijte příkazy IBM MQ (MQSC), jak je uvedeno v následujícím příkladu:

```
DEFINE QLOCAL(QM2) DESCR('Transmission queue to QM2') +
USAGE(XMITQ) QSGDISP(SHARED) +
CFSTRUCT(APPLICATION1) INITQ(SYSTEM.CHANNEL.INITQ) +
TRIGGER TRIGDATA(QSG.TO.QM2)
```

Agenti kanálů zpráv pro skupiny sdílení front

Kanál může být na inicializátoru kanálu spuštěn pouze v případě, že má přístup k definici kanálu pro kanál s tímto názvem.

Agent oznamovacího kanálu je program IBM MQ , který řídí odesílání a příjem zpráv. Agenti kanálu zpráv přesouvají zprávy z jednoho správce front do jiného; na každém konci kanálu je jeden agent kanálu zpráv.

Definice kanálu může být definována jako soukromá pro správce front nebo je uložena ve sdíleném úložišti a je k dispozici kdekoli (definice skupiny). To znamená, že kanál definovaný skupinou je k dispozici u všech inicializátorů kanálu ve skupině sdílení front.

Poznámka: Soukromá kopie definice skupiny může být změněna nebo odstraněna.

Chcete-li vytvořit definice kanálů skupiny, použijte příkazy IBM MQ (MQSC), jak je uvedeno v následujících příkladech:

```
DEFINE CHL(QSG.TO.QM2) CHLTYPE(SDR) +
TRPTYPE(TCP) CONNAME(QM2.MACH.IBM.COM) +
XMITQ(QM2) QSGDISP(GROUP)
```

```
DEFINE CHL(QM2.TO.QSG) CHLTYPE(RCVR) TRPTYPE(TCP) +
QSGDISP(GROUP)
```

Existují dvě perspektivy, ze kterých se můžete podívat na agenty kanálů zpráv použité pro distribuované řazení do front se skupinami sdílení front:

Příchozí

Příchozí kanál je sdílený kanál, je-li připojen ke správci front prostřednictvím skupinového modulu listener. Je připojen buď prostřednictvím generického rozhraní ke skupině sdílení front, a poté přeměrován na správce front v rámci skupiny nebo zacílený na port skupiny specifického správce front nebo název-lume používaný modulem listener skupiny.

Odchozí

Odchozí kanál je sdílený kanál, pokud přesouvá zprávy ze sdílené přenosové fronty. V ukázkových příkazech je odesílací kanál QSG . TO . QM2 sdíleným kanálem, protože jeho přenosová fronta QM2 je definována s QSGDISP (SHARED).

Fronta synchronizace pro skupiny sdílení front

Sdílené kanály mají svou vlastní sdílenou synchronizační frontu s názvem SYSTEM.QSG.CHANNEL.SYNCQ.

Tato synchronizační fronta je přístupná pro všechny členy skupiny sdílení front. (Soukromé kanály nadále používají soukromou synchronizační frontu. Viz [“Definování objektů IBM MQ”](#) na stránce 592). To znamená, že kanál může být restartován v jiném správci front a instanci inicializátoru kanálu v rámci skupiny sdílení front v případě selhání komunikačního subsystému, inicializátoru kanálu nebo správce front. Další informace uvádí téma [“Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front”](#) na stránce 614.

DQM se skupinami sdílení front vyžaduje, aby byla sdílená fronta k dispozici s názvem SYSTEM.QSG.CHANNEL.SYNCQ. Tato fronta musí být k dispozici, aby mohl být modul listener skupiny úspěšně spuštěn.

Pokud se modul listener skupiny nezdaří, protože fronta nebyla k dispozici, může být definována fronta a modul listener lze restartovat bez restartování inicializátoru kanálu. Nesdílené kanály nejsou ovlivněny.

Ujistěte se, že jste definovali tuto frontu pomocí INDXTYPE (MSGID). Tato definice zvyšuje rychlost, jakou lze přistupovat ke zprávám ve frontě.

Klastry a skupiny sdílení front

Sdílenou frontu můžete zpřístupnit pro klastr v jediné definici. Chcete-li tak učinit, zadejte při definování sdílené fronty název klastru.

Uživatelé v síti vidí sdílenou frontu jako hostitele každého správce front v rámci skupiny sdílení front. (Sdílená fronta není inzerována tak, že je hostována skupinou sdílení front). Klienti mohou spouštět relace se všemi členy skupiny sdílení front a vkládat zprávy do stejné sdílené fronty.

Další informace viz [“Konfigurace klastru správce front”](#) na stránce 216.

Kanály a serializace

Během partnerské obnovy sdílené fronty zpráv kanálu zpráv, které zpracovávají zprávy ve sdílených frontách, serializuje jejich přístup k frontám.

Pokud správce front ve skupině sdílení front selže, zatímco agent kanálu zpráv pracuje s nepotvrzenými zprávami v jedné nebo více sdílených frontách, bude kanál a přidružený inicializátor kanálu ukončen a pro správce front dojde k zotavení sdílené fronty typu peer.

Vzhledem k tomu, že partnerská obnova sdílené fronty je asynchronní činnost, může se zotavení partnerského kanálu pokusit o restartování kanálu v jiné části skupiny sdílení front před dokončením zotavení sdílené fronty typu peer. Pokud se tato událost stane, mohou být potvrzené zprávy zpracovány před tím, než se zprávy stále zotavují. Chcete-li se ujistit, že zprávy nejsou tímto způsobem zpracovány, agenti kanálu zpráv, kteří zpracovávají zprávy ve sdílených frontách, serializují jejich přístup k těmto frontám.

Pokus o spuštění kanálu, pro který stále probíhá obnova sdílené fronty zpráv, může vést k selhání. Bude vydána chybová zpráva oznamující, že zotavení probíhá, a kanál je uveden do stavu opakování. Jakmile je obnova typu peer správce front dokončena, kanál se může restartovat při následujícím opakování.

Pokus o RESOLVE, PING nebo DELETE kanálu může selhat ze stejného důvodu.

Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení zadané v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby připojení bylo definováno a k dispozici.

Vyberte si z jednoho ze dvou typů komunikačního protokolu, který lze použít:

- [TCP](#)
- [LU 6.2 až APPC/MVS](#)

Může být užitečné se podívat na volbu [Příklad konfigurace- IBM MQ for z/OS pomocí skupin sdílení front](#).

Definování připojení TCP pro skupiny sdílení front

Chcete-li definovat připojení TCP pro skupinu sdílení front, musí být nakonfigurovány určité atributy na odesílajícím a přijímajícím ukončení.

Informace o nastavení protokolu TCP naleznete v tématu [“Definování připojení TCP na systému z/OS”](#) na stránce 611.

Odesílání: Konec

Pole názvu připojení (CONNAME) v definici kanálu pro připojení k vaší skupině sdílení front musí být nastaveno na generické rozhraní skupiny sdílení front (viz [Skupiny sdílení front](#)). Další informace naleznete v tématu [Použití distributoru prostředí sysplex](#).

Příjem na TCP pomocí skupiny sdílení front

Příjem sdílených programů kanálu je spuštěn jako odezva na požadavek na spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn modul listener ke zjištění příchozích síťových požadavků a spuštění přidruženého kanálu. Tento program listener můžete spustit pomocí příkazu START LISTENER, s použitím příchozí odebrání skupiny nebo pomocí operací a řídicích panelů.

Všechny listenery skupin ve skupině sdílení front musí naslouchat na stejném portu. Máte-li více než jeden inicializátor kanálu běžící na jednom obrazu MVS, můžete definovat virtuální IP adresy a spustit program TCP listener pouze na určité adrese nebo názvu hostitele zadáním IPADDR v příkazu START LISTENER. (Další informace viz [START LISTENER](#).)

Definování připojení LU 6.2 na systému z/OS

Chcete-li definovat připojení LU 6.2 pro skupinu sdílení front, musí být nakonfigurovány určité atributy na odesílajícím a přijímajícím ukončení.

Informace o nastavení APPC/MVS naleznete v tématu [Nastavení komunikace pro z/OS](#).

Připojování k APPC/MVS (LU 6.2)

Pole názvu připojení (CONNAME) v definici kanálu pro připojení k vaší skupině sdílení front musí být nastaveno na symbolický název cíle, jak je uvedeno v datové sadě informací o připojení pro APPC/MVS. Partnerská LU uvedená v tomto symbolickém cíli musí být generický název prostředku. Další informace najdete v tématu [Definování do sítě pomocí generických prostředků](#).

Příjem na LU 6.2 pomocí generického rozhraní

Příjem sdílených MCA se spouští jako odezva na požadavek spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn program skupinového modulu listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Program modulu listener je server APPC/MVS. Spustíte ji pomocí příkazu START LISTENER, s použitím příchozí skupiny odebrání nebo pomocí operací a řídicích panelů. Je třeba určit název jednotky LU pro použití symbolického názvu místa určení definovaného v datové sadě informací o připojení. Další informace najdete v tématu [Definování do sítě pomocí generických prostředků](#).

Použití IBM MQ s IMS

Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

Chcete-li nakonfigurovat produkty IBM MQ a IMS pro spolupráci, je třeba provést následující úlohy:

- [“Nastavení adaptéru IMS”](#) na stránce 620
- [“Nastavení mostu IMS”](#) na stránce 626

Související pojmy

[“Konfigurace správců front v systému z/OS”](#) na stránce 523

Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

[“Použití IBM MQ s CICS”](#) na stránce 627

Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge.

[“Použití uživatelských procedur OTMA v produktu IMS” na stránce 630](#)

Toto téma použijte v případě, že chcete použít uživatelské procedury IMS Open Transaction Manager Access s IBM MQ for z/OS.

Související odkazy

[“Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services” na stránce 627](#)

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

Související informace

[IBM MQa IMS](#)

[Aplikace mostu IMS a IMS v systému IBM MQ for z/OS](#)

Nastavení adaptéru IMS

Použití produktu IBM MQ v rámci struktury IMS vyžaduje adaptér IBM MQ - IMS (obecně nazývaný jako adaptér IMS).

Toto téma obsahuje informace o tom, jak lze adaptér IMS zpřístupnit pro subsystém IMS. Pokud nejste obeznámeni s přizpůsobením subsystému IMS, přečtěte si téma *Informace o produktu IMS v příručce IBM Documentation*.

Chcete-li zpřístupnit adaptér IMS aplikacím produktu IMS, postupujte takto:

1. Define IBM MQ to IMS as an external subsystem using the IMS external subsystem attach facility (ESAF).

Viz [“Definování IBM MQ na IMS” na stránce 621](#).

2. Do souboru JOBLIB nebo STEPLIB ve zřetězení JOBLIB nebo STEPLIB zahrňte do souboru JCL pro řídicí oblast IMS a pro všechny závislé oblasti, které se připojí k produktu IBM MQ (pokud není v LPA nebo seznamu odkazů), vložte zaváděcí knihovnu IBM MQ thlqual.SCSQAUTH do souboru JOBLIB nebo STEPLIB. Není-li vaše knihovna JOBLIB nebo STEPLIB autorizována, zahrňte ji do zřetězení DFSESL za knihovnu obsahující moduly IMS (obvykle IMS RESLIB).

Zahrňte také thlqual.SCSQANLx (kde x je jazykový dopis).

Je-li DFSESL přítomen, pak je třeba do zřetězení přidat SCSQAUTH a SCSQANLx nebo přidat do LNKLIST. Přidání do zřetězení STEPLIB nebo JOBLIB v souboru JCL není dostatečné.

3. Okopírujte program IBM MQ assembler CSQQDEFV z thlqual.SCSQASMS do uživatelské knihovny.
4. Dodaný program CSQQDEFV obsahuje jeden název subsystému CSQ1 identifikované jako výchozí s tokenem jazyka IMS (LIT) produktu MQM1. Tento název můžete uchovat pro testování a verifikaci instalace.

Pro produkční subsystémy změňte hodnotu NAME=CSQ1 na své vlastní jméno podsystému, nebo použijte CSQ1. Podle potřeby můžete přidat další definice subsystému. Další informace o LITs najdete v tématu [“Definování správců front IBM MQ na adaptér IMS” na stránce 624](#).

5. Sestavte a propojte program za účelem vytvoření zaváděcího modulu CSQQDEFV. Pro sestavení přidejte do zřetězení SYSLIB knihovnu thlqual.SCSQMACS; použijte parametr link-edit RENT. Tato hodnota je zobrazena v ukázkovém JCL v souboru thlqual.SCSQPROC(CSQ4DEFV).
6. Zahrňte uživatelskou knihovnu obsahující modul CSQQDEFV, který jste vytvořili ve zřetězení JOBLIB nebo STEPLIB v souboru JCL pro libovolnou závislou oblast, která se připojuje k produktu IBM MQ. Umístěte tuto knihovnu před objekt SCSQAUTH, protože modul SCSQAUTH má nastaven výchozí modul načítání. Pokud toto neuděláte, obdržíte uživatele 3041abend od IMS.
7. Pokud adaptér IMS zjistí neočekávanou chybu IBM MQ, vyšle výpis paměti z/OS SNAP do názvu DD CSQSNAP a vydá aplikaci kód příčiny příčiny MQRC_UNEXPECTED_ERROR. Pokud příkaz CSQSNAP DD nebyl v kódu JCL oblasti závislé na IMS, nebude proveden žádný výpis paměti. Pokud k tomu dojde, můžete do JCL zahrnout příkaz CSQSNAP DD a znovu spustit aplikaci. Protože však některé problémy mohou být občasné, doporučuje se zahrnout příkaz CSQSNAP DD, abyste zachytili příčinu selhání v době, kdy k němu dojde.
8. Chcete-li použít dynamické volání IBM MQ (popsané v části [Dynamicky volat stubu IBM MQ](#)), sestavte dynamický stub, jak ukazuje [Obrázek 107 na stránce 621](#).

9. Chcete-li použít monitor spouštěčů produktu IMS , definujte monitor spouštěčů produktu IMS CSQQTRMN a proveďte příkazy PSBGEN a ACBGEN. Viz “Nastavení monitoru spouštěčů IMS” na stránce 625.
10. Pokud používáte produkt RACF k ochraně prostředků ve třídě OPERCMDS, ujistěte se, že ID uživatele přidružené k adresnímu prostoru správce front produktu IBM MQ má oprávnění k vydání příkazu MODIFY pro libovolný systém IMS , ke kterému se může připojit.

```
//DYNSTUB EXEC PGM=IEWL,PARM='RENT,REUS,MAP,XREF'
//SYSPRINT DD SYSOUT=*
//ACSQMOD DD DISP=SHR,DSN=thlqual.SCSQLOAD
//IMSLIB DD DISP=SHR,DSN=ims.reslib
//SYSLMOD DD DISP=SHR,DSN=private.load1
//SYSUT1 DD UNIT=SYSDA,SPACE=(CYL,1)
//SYSLIN DD *
INCLUDE ACSQMOD(CSQSTUB)
INCLUDE IMSLIB(DFSII000)
ALIAS MQCONN,MQCONN,MQDISC MQI entry points
ALIAS MQGET,MQPUT,MQPUT1 MQI entry points
ALIAS MQOPEN,MQCLOSE MQI entry points
ALIAS MQBACK,MQCMIT MQI entry points
ALIAS CSQBBAK,CSQBCMT MQI entry points
ALIAS MQINQ,MQSET MQI entry points
ALIAS DFSPLI,PLITDLI IMS entry points
ALIAS DFSCOBOL,CBLTDLI IMS entry points
ALIAS DFSFOR,FORTDLI IMS entry points
ALIAS DFSASM,ASMTDLI IMS entry points
ALIAS DFSPASCL,PASTDLI IMS entry points
ALIAS DFHEI01,DFHEI1 IMS entry points
ALIAS DFSAIBLI,AIBTDLI IMS entry points
ALIAS DFSESS,DSNCLI,DSNHLI IMS entry points
ALIAS MQCRTMH,MQDLTMH,MQDLTMP IMS entry points
ALIAS MQINQMP,MQSETMP,MQMHBUFF,MQBUFMH IMS entry points
MODE AMODE(31),RMODE(24) Note RMODE setting
NAME CSQQDYNS(R)
/*
```

¹Specify the name of a library accessible to IMS applications that want to make dynamic calls to WebSphere MQ.

Obrázek 107. Ukázka skriptu JCL pro propojení-úprava stubu dynamického volání

Související pojmy

“Nastavení mostu IMS” na stránce 626

Most IBM MQ - IMS je volitelná komponenta, která umožňuje IBM MQ vstupu a výstupu do a z existujících programů a transakcí, které nejsou IBM MQ-enabled.

Související informace

[IBM MQa IMS](#)

[Aplikace mostu IMS a IMS v systému IBM MQ for z/OS](#)

Definování IBM MQ na IMS

IBM MQ musí být definován pro řídicí oblast IMS a pro každou závislou oblast přistupujícího ke správci front IBM MQ . Chcete-li to provést, musíte v produktu IMS vytvořit člena subsystému (SSM).Knihovna PROCLIB a identifikujte SSM v příslušných regionech IMS .

Umístění položky člena subsystému do IMS.PROCLIB

Každá položka SSM v produktu IMS.PROCLIB definuje připojení z regionu produktu IMS k jinému správci front.

To name an SSM, concatenate the value (one to four alphanumeric characters) of the IMSID field of the IMS IMCTRL macro with any name (one to four alphanumeric characters) defined by your site.

Jeden SSM může být sdílen všemi regiony IMS nebo může být definován specifický člen pro každý region. Tento člen obsahuje tolik položek, jako jsou připojení k externím subsystémům. Každá položka je záznam o délce 80 znaků.

Poziční parametry

Pole v této položce jsou:

SSN, LIT, ESMT, RTT, REO, CRC

kde:

SSN

Určuje název správce front produktu IBM MQ. Je to povinné a musí obsahovat jeden až čtyři znaky.

LIT

Určuje token jazykového rozhraní (LIT-Language Interface Token) dodaný produktu IMS. Toto pole je povinné, jeho hodnota se musí shodovat s hodnotou v modulu CSQQDEFV.

ESMIT

Uvádí tabulku modulu externího subsystému (ESMT). Tato tabulka určuje, které moduly příloh musí být načteny produktem IMS. CSQQESMT je požadovaná hodnota pro toto pole.

RTTŮV

Tato volba není podporována produktem IBM MQ.

REO

Uvádí volbu chyby regionu (REO), která se má použít, pokud aplikace IMS odkazuje na jiný než operační externí subsystém nebo pokud nejsou prostředky k dispozici při vytváření času podprocesu. Toto pole je volitelné a obsahuje jeden znak, který může být:

R

Předává návratový kód aplikaci, což označuje, že požadavek na služby IBM MQ selhal.

Q

Ukončí aplikaci s kódem nestandardního ukončení U3051, zálohují aktivitu na poslední bod potvrzení, provede operaci PSTOP pro transakci a znovu odešle vstupní zprávu. Tato volba se používá pouze tehdy, když se aplikace IMS pokouší odkazovat na jiný než operační externí subsystém, nebo pokud nejsou prostředky k dispozici při vytváření času podprocesu.

IBM MQ a kódy příčiny jsou vráceny aplikaci, pokud se problém IBM MQ vyskytne, zatímco IBM MQ zpracovává požadavek; to znamená poté, co adaptér předal požadavek na IBM MQ.

A

Ukončí aplikaci s kódemabend U3047 a zahodí vstupní zprávu. Tato volba se používá pouze v případě, že aplikace IMS odkazuje na jiný než operační externí subsystém, nebo pokud jsou prostředky nedostupné při vytváření času podprocesu.

IBM MQ a kódy příčiny jsou vráceny aplikaci, pokud se problém IBM MQ vyskytne, zatímco IBM MQ zpracovává požadavek; to znamená poté, co adaptér předal požadavek na IBM MQ.

CRC

Tato volba může být uvedena, ale není použita IBM MQ.

Poznámka: Podrobné informace o všech pozičních parametrech najdete v tématu [Jak jsou externí subsystémy zadány do systému IMS](#).

Příklad záznamu SSM je:

CSQ1, MQM1, CSQQESMT, , R,

kde:

- CSQ1** Výchozí název subsystému, jak je dodáván s IBM MQ. Tento stav můžete změnit, aby vyhovoval vaší instalaci.
- MQM1** Výchozí hodnota LIT, jak je dodána v CSQQDEFV.
- CSQQESMT** Název modulu externího subsystému. Tuto hodnotu musíte použít.
- R** Volba REO.

Parametry klíčových slov

Parametry IBM MQ lze zadat ve formátu klíčových slov; chcete-li to provést, je třeba zadat SST=Db2. Ostatní parametry jsou popsány v části [Poziční parametry](#) jsou zobrazeny v následujícím příkladu:

```
SST=DB2,SSN=SYS3,LIT=MQM3,ESMT=CSQQESMT
```

kde:

- SYS3** Název subsystému
- MQM3** LIT, jak je uvedeno v CSQQDEFV
- CSQQESMT** Název modulu externího subsystému

Uvedení parametru EXEC SSM

Uvedte parametr EXEC SSM ve spouštěcí proceduře řídicí oblasti IMS. Tento parametr uvádí jeden znak pro čtyřznakový název člena subsystému (SSM).

Uvedete-li SSM pro řídicí oblast IMS, jakýkoli závislý region spuštěný pod řídicí oblastí se může připojit ke správci front IBM MQ uvedenému v IMS. Člen PROCLIB uvedený v parametru SSM. IMS. Název členu PROCLIB je ID IMS (IMSID= *xxxx*) zřetěžené s jedním až čtyřmi znaky zadanými v parametru EXEC SSM. ID IMS je parametr ID IMSmakra generování CTRL IMS.

Produkt IMS umožňuje definovat tolik externích připojení k subsystému, jak je požadováno. Pro různé správce front IBM MQ může být definováno více než jedno připojení. Všechna spojení typu IBM MQ musí být ve stejném systému z/OS. Pro závislou oblast můžete uvést závislý region SSM nebo použít tu, který je uvedený pro řídicí region. Můžete uvést různé volby chyby oblasti (REO) v nezávislé SSM oblasti a v řídicí oblasti SSM. [Tabulka 49 na stránce 623](#) zobrazuje různé možnosti specifikací SSM.

SSM pro řídicí oblast	SSM pro závislý region	Akce	Komentáře
Ne	Ne	Není	Žádný externí subsystém nemůže být připojen.
Ne	Ano	Není	Žádný externí subsystém nemůže být připojen.
Ano	Ne	Použít řídicí oblast SSM	Aplikace naplánované v oblasti mohou přistupovat k externím subsystémům označeným v řídicím regionu SSM. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do oblasti řídicí oblasti a adresních prostorů závislých oblastí.
Ano	Ano (prázdné)	Pro závislý region není použit žádný SSM.	Aplikace naplánované v této oblasti mohou přistupovat pouze k databázím DL/I. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do adresního prostoru řídicí oblasti.

Tabulka 49. Volby specifikace SSM (pokračování)

SSM pro řídicí oblast	SSM pro závislý region	Akce	Komentáře
Ano	Ano (není prázdné)	Zkontrolujte SSM závislé oblasti s kontrolní oblastí SSM	Aplikace naplánované v této oblasti mohou přistupovat pouze k externím subsystémům, které jsou identifikovány v obou systémech SSM. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do oblasti řídicí oblasti a adresních prostorů závislých oblastí.

Neexistuje žádný specifický parametr k řízení maximálního počtu možností specifikace SSM.

Přednačítání adaptéru IMS

Výkonnost adaptéru IMS lze zlepšit, pokud je předem načtena pomocí IMS. Předložení je řízeno členem DFSMPLxx IMS.PROCLIB: viz "IMS Administration Guide: System", kde získáte další informace. Názvy modulů IBM MQ, které mají být zadány, jsou:

CSQACLST	CSQAMLST	CSQAPRH	CSQAVICM	CSQFSALM	CSQQDEFV
PŘIPOJENÍ CSQQCONN	CSQQDISC	CSQQTERM	CSQQINIT	CSQQBACK	CSQQCMMT
CSQQESMT	PŘÍPRAVA CSQQPREP	CSQQTTHD	ČEKÁNÍ CSQQWAIT	CSQQNORM	CSQQSSOQNA ME
CSQQSSON	CSQFSTAB	CSQQRESV	CSQQSNAP	CSQQCMND	CSQCVER
CSQQTMID	CSQQTRGI	CSQQCON2	CSQBPAPI	CSQBCRMH	CSQBAPPL

Další informace o použití příkazu IBM MQ classes for JMS naleznete v tématu [Použití produktu IBM MQ classes for JMS v systému IMS](#).

Aktuální verze produktu IMS podporují předběžné načítání modulů IBM MQ z knihoven formátu PDS-E pouze v regionech MPP, BMP, IFP, JMP a JBP. Jakýkoli jiný typ oblasti IMS nepodporuje předběžné načítání z knihoven PDS-E. Je-li pro jakýkoli jiný typ oblasti vyžadováno předběžné načítání, musí být zadané moduly produktu IBM MQ zkopírovány do knihovny formátu PDS.

Definování správců front IBM MQ na adaptér IMS

Názvy správců front produktu IBM MQ a jejich odpovídající tokeny jazykového rozhraní (LITs) musí být definovány v tabulce definic správce front.

Použijte dodané makro CSQQDEFX k vytvoření zaváděcího modulu CSQQDEFV. [Obrázek 108 na stránce 624](#) ukazuje syntaxi tohoto makra assembleru.

```
CSQQDEFX TYPE=ENTRY|DEFAULT, NAME=qmgr-name, LIT=token
or
CSQQDEFX TYPE=END
```

Obrázek 108. Syntaxe makra CSQQDEFX

Parametry

TYP=POLOŽKA|VÝCHOZÍ

Uveďte buď TYPE=ENTRY, nebo TYPE=DEFAULT takto:

TYP=POLOŽKA

Určuje, že má být vygenerována položka tabulky popisující správce front IBM MQ , který je k dispozici pro aplikaci produktu IMS . Pokud se jedná o první položku, vygeneruje se také záhlaví tabulky, včetně příkazu CSQQDEFV CSECT.

TYP=VÝCHOZÍ

Jako pro TYP=POLOŽKA. Uvedený správce front je výchozím správcem front, který má být použit, když MQCONN nebo MQCONNX uvádí název, který je prázdný. V tabulce musí být pouze jeden takový záznam.

JMÉNO= *qmgr-name*

Uvádí název správce front, jak je uvedeno spolu s MQCONN nebo MQCONNX .

LIT = *token*

Určuje název tokenu jazyka jazyka (LIT), který produkt IMS používá k identifikaci správce front.

Volání MQCONN nebo MQCONNX přidruží vstupní parametr *name* a výstupní parametr *hconn* s popiskem názvu, a tedy LIT v záznamu CSQQDEFV. Další volání příkazu IBM MQ , která předává parametr *hconn* , používá LIT z položky CSQQDEFV identifikované ve volání MQCONN nebo MQCONNX k přímým voláním správce front produktu IBM MQ definovaného v rámci člena SSM produktu IMS PROCLIB se stejným LIT.

Stručně řečeno, parametr *name* na volání MQCONN nebo MQCONNX identifikuje LIT v CSQQDEFV a stejné logické části LIT v členu SSM identifikuje správce front IBM MQ . (Informace o volání MQCONN naleznete v tématu [MQCONN-Připojit správce front](#). Informace o volání MQCONNX viz [MQCONNX-Connect queue manager \(extended\)](#).)

TYP=KONEC

Určuje, že tabulka je úplná. Je-li tento parametr vynechán, předpokládá se parametr TYPE=ENTRY.

Použití makra CSQQDEFX

Obrázek 109 na stránce 625 zobrazuje obecné rozvržení tabulky definic správce front.

```
CSQQDEFX NAME=subsystem1,LIT=token1
CSQQDEFX NAME=subsystem2,LIT=token2,TYPE=DEFAULT
CSQQDEFX NAME=subsystem3,LIT=token3
...
CSQQDEFX NAME=subsystemN,LIT=tokenN
CSQQDEFX TYPE=END
END
```

Obrázek 109. Rozvržení tabulky definic správce front

Nastavení monitoru spouštěčů IMS

Chcete-li monitorovat inicializační frontu IBM MQ , můžete nastavit dávkově orientovaný program IMS .

Definujte aplikaci pro IMS pomocí modelu CSQQTAPL v knihovně thlqual.SCSQPROC (viz [Příklad definice transakce pro CSQQTRMN](#)).

Generujte PSB a ACB za použití modelu CSQQTPSB v knihovně thlqual.SCSQPROC (viz [Příklad definice PSB pro CSQQTRMN](#)).

```
* This is the application definition *
* for the IMS Trigger Monitor BMP   *
```

```
APPLCTN PSB=CSQQTRMN,
PGMTYPE=BATCH,
SCHDTYP=PARALLEL
```

Obrázek 110. Příklad definice transakce pro CSQQTRMN

```
PCB TYPE=TP,          ALTPCB for transaction messages
MODIFY=YES,           To "triggered" IMS transaction
PCBNAME=CSQQTRMN
PCB TYPE=TP,          ALTPCB for diagnostic messages
MODIFY=YES,           To LTERM specified or "MASTER"
PCBNAME=CSQQTRMG,
EXPRESS=YES
PSBGEN LANG=ASSEM,
PSBNAME=CSQQTRMN,    Runs program CSQQTRMN
CMPAT=YES
```

Obrázek 111. Příklad definice PSB pro CSQQTRMN

Další informace o spuštění a zastavení monitoru spouštěčů IMS naleznete v tématu [Ovládání monitoru spouštěčů IMS](#).

Nastavení mostu IMS

Most IBM MQ - IMS je volitelná komponenta, která umožňuje IBM MQ vstupu a výstupu do a z existujících programů a transakcí, které nejsou IBM MQ-enabled.

Toto téma popisuje, co je třeba udělat pro přizpůsobení mostu IBM MQ - IMS .

Definujte parametry XCF a OTMA pro IBM MQ.

Tento krok definuje názvy skupin a členů XCF pro váš systém IBM MQ a další parametry OTMA. IBM MQ a IMS musí patřit do stejné skupiny XCF. Použijte klíčové slovo OTMACON makra CSQ6SYSP , abyste přizpůsobili tyto parametry v modulu zátěže parametrů systému.

Další informace najdete v tématu [Použití CSQ6SYSP](#) .

Definujte parametry XCF a OTMA pro IMS.

Tento krok definuje názvy skupin a členů XCF pro systém IMS . IMS a IBM MQ musí patřit do stejné skupiny XCF.

Přidejte následující parametry do svého seznamu parametrů IMS , buď ve vašem JCL, nebo v členu DFSPBxxx v IMS PROCLIB:

OTMA=Y

Tím se spustí OTMA automaticky při spuštění produktu IMS . (Je volitelný, pokud zadáte OTMA=N, můžete také spustit OTMA zadáním příkazu IMS /START OTMA.)

GRNAME =

Tento parametr poskytuje název skupiny XCF.

Je to stejné jako název skupiny uvedený v definici třídy úložiště (viz další krok) a v parametru Group v klíčovém slově OTMACON makra CSQ6SYSP .

OTMANM =

Tento parametr udává název člena XCF systému IMS .

To je stejné jako jméno členu uvedené v definici třídy ukládání (viz další krok).

Řekněte IBM MQ skupině XCF a názvu člena systému IMS .

Toto je určeno třídou úložiště fronty. Chcete-li odesílat zprávy přes most IBM MQ - IMS , musíte je zadat při definování třídy úložiště pro frontu. Ve třídě úložiště musíte definovat skupinu XCF a název člena cílového systému IMS . Chcete-li to provést, použijte buď operace IBM MQ a ovládací panely , nebo použijte příkazy IBM MQ , jak je popsáno v části [Úvod do formátu programových příkazů](#).

Nastavte zabezpečení, které požadujete.

Příkaz /SECURE OTMA IMS určuje úroveň zabezpečení, která má být použita pro **každý** IBM MQ správce front, který se připojuje k produktu IMS prostřednictvím modulu OTMA. Další informace najdete v tématu [Aspekty zabezpečení pro použití produktu IBM MQ s produktem IMS](#) .

Přidání dalšího připojení produktu IMS ke stejnému správci front

Chcete-li přidat připojení produktu IMS ke stejnému správci front, je třeba provést následující akce:

- Definujte druhou paměťovou třídu [STGCLASS](#) tak, aby ukazovala na nový objekt IMS; další informace viz [DEFINE STGCLASS](#) .
- Přidejte novou lokální frontu, která bude ukazovat na druhou třídu ukládání.

Důležité:

- Jedna lokální fronta nemůže ukazovat na dvě paměťové třídy.
- Jedna paměťová třída nemůže ukazovat na dva mosty IMS .
- IBM MQ a IMS musí patřit do stejné skupiny XCF. Použijte klíčové slovo OTMACON makra CSQ6SYSP , abyste přizpůsobili tyto parametry v modulu zátěže parametrů systému.

Další informace najdete v tématu [Použití CSQ6SYSP](#) .

Související pojmy

[“Nastavení adaptéru IMS” na stránce 620](#)

Použití produktu IBM MQ v rámci struktury IMS vyžaduje adaptér IBM MQ - IMS (obecně nazývaný jako adaptér IMS).

Související informace

[IBM MQa IMS](#)

[Aplikace mostu IMS a IMS v systému IBM MQ for z/OS](#)

Použití IBM MQ s CICS

Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge .

Další informace o konfiguraci adaptéru IBM MQ CICS a komponent produktu IBM MQ CICS bridge naleznete v části [Konfigurace připojení k produktu MQ v dokumentaci produktu CICS](#) .

Související pojmy

[“Použití IBM MQ s IMS” na stránce 619](#)

Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

Související odkazy

[“Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services” na stránce 627](#)

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

Související informace

[IBM MQ a CICS](#)

Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

Následující tabulky ukazují, co je třeba provést v produktu IBM MQ for z/OS , pokud upgradujete svou úroveň nebo používáte službu na tyto produkty:

- Jazykové prostředí
- z/OS Volatelné služby (například APPC a RRS)

<i>Tabulka 50. Služba byla použita nebo byl produkt upgradován na nové vydání</i>		
Produkt	Akce při použití CALLLIBS a SMP/E V3r2 nebo novější Poznámka: Pro Jazykové prostředí a Callable Services nemusíte spouštět samostatné úlohy. Jedna práce bude stačit.	Akce při použití SPOJE
Jazykové prostředí	<ol style="list-style-type: none"> 1. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 2. Na kartě SMP_CNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace najdete v tématu <i>SMP/E for z/OS: Commands</i> . 3. Spusťte úlohu SMP/E. 	Nebyla požadována žádná akce za předpokladu, že jsou zóny SMP/E nastaveny pro automatické opětovné propojení, a úloha CSQ8SLDQ byla spuštěna.
Volatelné služby	<ol style="list-style-type: none"> 1. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 2. Na kartě SMP_CNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace najdete v tématu <i>SMP/E for z/OS: Commands</i> . 3. Spusťte úlohu SMP/E. 	Nebyla požadována žádná akce za předpokladu, že jsou zóny SMP/E nastaveny pro automatické opětovné propojení, a úloha CSQ8SLDQ byla spuštěna.

Tabulka 51. Jeden z produktů byl aktualizován na nové vydání v novém prostředí SMP/E a v knihovnách

Produkt	Akce při použití CALLLIBS a SMP/E V3r2 nebo novější	Akce při použití SPOJE
Jazykové prostředí	<p>Poznámka: Nemusíte spouštět tři samostatné úlohy pro Jazykové prostředí a Callable services. Pro oba produkty bude stačit jedna úloha.</p> <ol style="list-style-type: none"> 1. Změňte položky DDDEF pro SCEELKED a SCEESPC tak, aby ukazovala na novou knihovnu. 2. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 3. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace najdete v tématu <i>SMP/E for z/OS: Commands</i>. 4. Spusťte úlohu SMP/E. 	<ol style="list-style-type: none"> 1. Odstraňte dílčí položky XZMOD pro následující položky LMOD v cílové zóně IBM MQ for z/OS : CMQXDCST, CMQXRCTL, CMQXSUPR, CSQCBE00, CSQCBE30, CSQCBP00, CSQCBP10, CSQCBR00, CSQUCVX, CSQUDLQH, CSQVXPCB, CSQVXSPT, CSQXDCST, CSQXRCTL, CSQXSUPR, CSQXTDMI, CSQXTCP, CSQXTNSV, CSQ7DRPS, IMQB23IC, IMQB23IM, IMQB23IR, IMQS23IC, IMQS23IM, IMQS23IR 2. Nastavte příslušné ZONEINDEXs mezi zónami IBM MQ a oblastmi jazykového prostředí. 3. Přizpůsobte CSQ8SLDQ tak, aby odkazovaly na novou zónu v parametru FROMZONE příkazů LINK. CSQ8SLDQ může být nalezen v knihovně SCSQINST. 4. Spusťte CSQ8SLDQ.
Volatelné služby	<ol style="list-style-type: none"> 1. Změňte DDDEF pro CSSLIB tak, aby ukazovala na novou knihovnu 2. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 3. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace najdete v tématu <i>SMP/E for z/OS: Commands</i>. 4. Spusťte úlohu SMP/E. 	<ol style="list-style-type: none"> 1. Odstraňte dílčí položky XZMOD pro následující položky LMOD v cílové zóně IBM MQ for z/OS : CMQXRCTL, CMQXSUPR, CSQBSRV, CSQILPLM, CSQXJST, CSQXRCTL, CSQXSUPR, CSQ3AMGP, CSQ3EPX, CSQ3REPL 2. Nastavte příslušnou hodnotu ZONEINDEXs mezi zónami IBM MQ a poli Volatelné služby. 3. Přizpůsobte CSQ8SLDQ tak, aby odkazovaly na novou zónu v parametru FROMZONE příkazů LINK. CSQ8SLDQ může být nalezen v knihovně SCSQINST. 4. Spusťte CSQ8SLDQ.

Příklad úlohy pro opětovné připojení modulů při použití volání CALLLIBS viz [“Spuštění úlohy LINKA CALLLIBS”](#) na stránce 629.

Spuštění úlohy LINKA CALLLIBS

Příklad úlohy pro opětovné propojení modulů při použití CALLLIBS.

Níže je uveden příklad úlohy pro opětovné propojení modulů při použití CALLLIBS na systému SMP/E V3r2 . Musíte poskytnout JOBCARD a název datové sady SMP/E CSI, které obsahuje IBM MQ for z/OS.

```

//*****
//* RUN LINK CALLLIBS.
//*****
//CALLLIBS EXEC PGM=GIMSMP,REGION=4096K
//SMPCSI DD DSN=your.csi
// DISP=SHR
//SYSPRINT DD SYSOUT=*
//SMPCNTL DD *
SET BDY(TZONE).
LINK LMODS CALLLIBS .
/*

```

Obrázek 112. Příklad úlohy SMP/E LINK CALLLIBS

Použití uživatelských procedur OTMA v produktu IMS

Toto téma použijte v případě, že chcete použít uživatelské procedury IMS Open Transaction Manager Access s IBM MQ for z/OS.

Chcete-li odeslat výstup z transakce produktu IMS do produktu IBM MQa tato transakce nepochází v produktu IBM MQ, je třeba vytvořit kód jedné nebo více uživatelských procedur produktu IMS OTMA.

Podobně, pokud chcete odesílat výstup do cíle mimo OTMA a transakce pochází z IBM MQ, musíte také kódovat jeden nebo více ukončovacích procedur IMS OTMA.

V produktu IMS jsou k dispozici následující uživatelské procedury, které umožňují přizpůsobit zpracování mezi produkty IMS a IBM MQ:

- Předvedení před směrováním OTMA
- Uživatelská procedura DRU (destination resolution user)

Názvy uživatelských procedur OTMA

Musíte pojmenovat výstupní bod předběžného směrování DFSYPRX0. Název DRU můžete pojmenovat cokoliv, dokud se nekoliduje s názvem modulu, který je již v produktu IMS.

Určení jména uživatelských procedur pro rozpoznávání místa určení

Můžete použít parametr *Druexit* klíčového slova OTMACON makra CSQ6SYSP k určení názvu uživatelské procedury OTMA DRU, která má být spuštěna produktem IMS.

Chcete-li zjednodušit identifikaci objektů, zvažte možnost přijetí konvence pojmenování DRU0xxxx, kde xxxx je název vašeho správce front IBM MQ .

Pokud neuvedete název ukončení DRU v parametru OTMACON, předvolba je DFSYDRU0. Ukázka tohoto modulu je dodávaná produktem IMS. Informace o tomto tématu naleznete v příručce *IMS/ESA Customization Guide* .

Konvence pojmenování pro místo určení IMS

Pro místo určení, do kterého chcete odeslat výstup z programu IMS , potřebujete konvenci pojmenování. Toto je cíl, který je nastaven v rámci volání CHNG vaší aplikace IMS , nebo který je přednastaven v PSB IMS .

Ukázkový scénář pro uživatelskou proceduru OTMA

Následující témata použijte jako příklad pro uživatelskou proceduru před směrováním a cílovou uživatelskou proceduru směrování pro produkt IMS:

- [“Ukončení před směrováním DFSYPRX0” na stránce 631](#)

- [“Uživatelská procedura rozpoznání místa určení” na stránce 632](#)

Chcete-li zjednodušit identifikaci, použijte místo určení OTMA podobné názvu správce front produktu IBM MQ , například název správce front produktu IBM MQ . V tomto případě, pokud je název správce front IBM MQ " **VCPE** ", cíl nastavený voláním CHNG je" **VCPEVCPE** ".

Související pojmy

[“Použití IBM MQ s IMS” na stránce 619](#)

Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

Související informace

[IBM MQa IMS](#)

[Aplikace mostu IMS a IMS v systému IBM MQ for z/OS](#)

Ukončení před směrováním DFSYPRX0

Toto téma obsahuje ukázkové ukončení před routing pro OTMA v produktu IMS.

Musíte nejprve kódovat předsměrovací ukončení DFSYPRX0. Parametry předané této rutině produktem IMS jsou dokumentovány v příručce *IMS/ESA Customization Guide*.

Tato uživatelská procedura testuje, zda je zpráva určena pro známé místo určení OTMA (v našem příkladu VCPEVCPE). Je-li tomu tak, výjezd musí zkontrolovat, zda transakce odesílající zprávu pocházela z OTMA. Pokud zpráva vznikla v OTMA, bude mít záhlaví OTMA, takže byste měli ukončit DFSYPRX0 s registrací 15 nastaveným na nulu.

- Pokud transakce odesílající zprávu nepochází v OTMA, musíte nastavit, aby byl název klienta platným klientem OTMA. Jedná se o člena XCF správce front produktu IBM MQ , do kterého chcete odeslat zprávu. Příručka *IMS/ESA Customization Guide* informuje o tom, kde nastavit tuto hodnotu. Navrhujeme, abyste nastavili název vašeho klienta (v parametru OTMACON makra CSQ6SYSP) je nastaven na název správce front. Toto nastavení je výchozí. Pak byste měli ukončit DFSYPRX0 nastavení registru 15 až 4.
- Pokud transakce odesílající zprávu pocházela z OTMA a místo určení je mimo OTMA, měli byste nastavit registr 15 na 8 a ukončit.
- Ve všech ostatních případech byste měli nastavit registr 15 na nulu.

Pokud nastavíte název klienta OTMA na název klienta, který není známý pro produkt IMS, bude volání CHNG nebo ISRT vracet stavový kód A1 .

Pro systém IMS , který komunikuje s více než jedním správcem front IBM MQ , byste měli opakovat logiku pro každého správce front IBM MQ .

Ukázkový assembler kód se zobrazí v [Obrázek 113 na stránce 632](#):

```

TITLE 'DFSYPRX0: OTMA PRE-ROUTING USER EXIT'
DFSYPRX0 CSECT
DFSYPRX0 AMODE 31
DFSYPRX0 RMODE ANY
*
SAVE (14,12),,DFSYPRX0&SYSDATE&SYSTIME
SPACE 2
LR R12,R15          MODULE ADDRESSABILITY
USING DFSYPRX0,R12
*
L   R2,12(,R1)      R2 -> OTMA PREROUTE PARMS
*
LA  R3,48(,R2)      R3 AT ORIGINAL OTMA CLIENT (IF ANY)
CLC 0(16,R3),=XL16'00' OTMA ORIG?
BNE OTMAIN          YES, GO TO THAT CODE
*
NOOTMAIN DS 0H      NOT OTMA INPUT
LA  R5,8(,R2)       R5 IS AT THE DESTINATION NAME
CLC 0(8,R5),=C'VCPEVCPE' IS IT THE OTMA UNSOLICITED DEST?
BNE EXIT0           NO, NORMAL PROCESSING
*
L   R4,80(,R2)      R4 AT ADDR OF OTMA CLIENT
MVC 0(16,R4),=CL16'VCPE' CLIENT OVERRIDE
B   EXIT4           AND EXIT
*
OTMAIN DS 0H        OTMA INPUT
LA  R5,8(,R2)       R5 IS AT THE DESTINATION NAME
CLC 0(8,R5),=C'VCPEVCPE' IS IT THE OTMA UNSOLICITED DEST?
BNE EXIT8           NO, NORMAL PROCESSING

*
EXIT0 DS 0H
LA  R15,0           RC = 0
B   BYEBYE
*
EXIT4 DS 0H
LA  R15,4           RC = 4
B   BYEBYE
*
EXIT8 DS 0H
LA  R15,8           RC = 8
B   BYEBYE
*
BYEBYE DS 0H
RETURN (14,12),,RC=(15) RETURN WITH RETURN CODE IN R15
SPACE 2
REQUATE
SPACE 2
END

```

Obrázek 113. Ukázka výstupního souboru sestavení OTMA před přesměrováním

Uživatelská procedura rozpoznání místa určení

Toto téma obsahuje ukázkou uživatelské procedury rozpoznání místa určení cíle pro produkt IMS.

Pokud jste nastavili registry 15 až 4 v DFSYPRX0, nebo pokud byl zdrojem transakce OTMA **a** jste nastavili registr 15 na nulu, je vyvolána uživatelská procedura DRU. V tomto příkladu je název uživatelské procedury DRU DRU0VCPE.

Uživatelská procedura DRU zkontroluje, zda je cílem VCPEVCPE. Je-li tomu tak, nastaví uživatelská data OTMA (v předponě OTMA) takto:

Offset

Uživatelská data OTMA

(dekadicky)

0

Délka uživatelských dat OTMA (v tomto příkladu, 334)

2

MQMD

326

Odpověďt na formát

Tyto odchylky jsou tam, kde most IBM MQ - IMS očekává, že tyto informace najde.

Navrhujeme, aby odchod z DRU byl tak jednoduchý, jak je to jen možné. Proto jsou v této ukázce všechny zprávy pocházející z produktu IMS pro určitého správce front produktu IBM MQ vloženy do stejné fronty IBM MQ .

Pokud musí být zpráva perzistentní, musí produkt IMS používat synchronizované propojení procesů transakcí. Pro tento úkol musí uživatelská procedura DRU nastavit příznak OUTPUT. Další podrobnosti naleznete v příručce *IMS/ESA Customization Guide*.

Chcete-li zpracovat tuto frontu a použít informace z struktury MQMD, struktury MQIIH (je-li k dispozici) nebo uživatelská data pro směrování každé zprávy do místa určení, napište aplikaci IBM MQ .

V produktu [Obrázek 114](#) na stránce [633](#) se zobrazí ukázka uživatelské procedury assembler DRU.

```
TITLE 'DRU0VCPE: OTMA DESTINATION RESOLUTION USER EXIT'
DRU0VCPE CSECT
DRU0VCPE AMODE 31
DRU0VCPE RMODE ANY
*
SAVE (14,12),,DRU0VCPE&SYSDATE&SYSTIME
SPACE 2
LR R12,R15          MODULE ADDRESSABILITY
USING DRU0VCPE,R12
*
L R2,12(,R1)        R2 -> OTMA DRU PARMS
*
L R5,88(,R2)        R5 ADDR OF OTMA USERDATA
LA R6,2(,R5)        R6 ADDR OF MQMD
USING MQMD,R6       AS A BASE
*
LA R4,MQMD_LENGTH+10 SET THE OTMA USERDATA LEN
STH R4,0(,R5)       = LL + MQMD + 8
*
MVI 0(R6),X'00'     ...NULL FIRST BYTE
MVC 1(255,R6),0(R6) ...AND PROPAGATE IT
MVC 256(MQMD_LENGTH-256+8,R6),255(R6) ...AND PROPAGATE IT
*
VCPE DS 0H
CLC 44(16,R2),=CL16'VCPE' IS DESTINATION VCPE?
BNE EXIT4          NO, THEN DEST IS NON-OTMA
MVC MQMD_REPLYTOQ,=CL48'IMS.BRIDGE.UNSOLICITED.QUEUE'
MVC MQMD_REPLYTOQMGR,=CL48'VCPE' SET QNAME AND QMGRNAME
MVC MQMD_FORMAT,MQFMT_IMS SET MQMD FORMAT NAME
MVC MQMD_LENGTH(8,R6),MQFMT_IMS_VAR_STRING
*
B EXIT0            SET REPLYTO FORMAT NAME
*
EXIT0 DS 0H
LA R15,0           SET RC TO OTMA PROCESS
B BYEBYE          AND EXIT
*
EXIT4 DS 0H
LA R15,4           SET RC TO NON-OTMA
B BYEBYE          AND EXIT
*
BYEBYE DS 0H
RETURN (14,12),,RC=(15) RETURN CODE IN R15
SPACE 2
REQUATE
SPACE 2
CMQA EQUONLY=NO
CMQMDA DSECT=YES
SPACE 2
END
```

Obrázek 114. Uživatelská procedura DRU assembler

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LICENČNÍ INFORMACE:

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

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

Informace o programovacím rozhraní

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

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

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

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

Ochranné známky

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

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

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

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

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

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



Číslo položky:

(1P) P/N: