7.5

Konfigurace produktu IBM WebSphere MQ

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 439.

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

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

Obsah

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 WebSphere MQsi přečtěte informace o koncepcích produktu IBM WebSphere MQ v příručce IBM WebSphere MQ Technical overview. Přečtěte si o tom, jak plánovat své prostředí IBM WebSphere MQ v Plánování .

Existuje řada různých metod, které můžete použít k vytvoření, konfiguraci a administraci správců front a jejich souvisejících prostředků v produktu IBM WebSphere 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 WebSphere MQ .

Pokyny, jak vytvořit, spustit, zastavit a odstranit správce front, naleznete v tématu “Vytváření a údržba správců front” na stránce 18.

Informace o tom, jak vytvořit komponenty potřebné k propojení vašich instalací a aplikací produktu IBM WebSphere MQ , najdete v tématu “Připojování aplikací pomocí distribuovaných front” na stránce 27.

Pokyny, jak připojit klienty k serveru IBM WebSphere MQ pomocí různých metod, najdete v tématu “Konfigurace připojení mezi klientem a serverem” na stránce 96.

Pokyny, jak nakonfigurovat klastr správců front, naleznete v části “Konfigurace klastru správce front” na stránce 156.

Chování produktu IBM WebSphere MQ nebo správce front můžete změnit změnou konfiguračních informací. Další informace viz “Změna konfiguračních informací IBM WebSphere MQ a správce front” na stránce 406. Obecně není třeba restartovat správce front, aby se změny konfigurace projevily, kromě případu, kdy je uvedena v této dokumentaci k produktu.

Související pojmy

Technický přehled produktu WebSphere MQ

Související úlohy

Správa lokálních objektů produktu WebSphere MQ

Správa vzdálených objektů produktu WebSphere MQ

Naplánování

Konfigurace více instalací v systému UNIX, Linux, and Windows

Používáte-li více instalací ve stejném systému, musíte nakonfigurovat instalace a správce front.

Tyto informace platí pro UNIX, Linux®, and Windows.

Při konfiguraci vašich instalací použijte informace v následujících odkazech:

- “Změna primární instalace” na stránce 15
- “Přidružení správce front k instalaci” na stránce 16
- “Připojování aplikací v prostředí s více instalačními prostředí” na stránce 6

Související pojmy

Více instalací

Související úlohy

Výběr primární instalace

Výběr názvu instalace

Připojování aplikací v prostředí s více instalačními prostředí

Pokud je v systémech UNIX, Linux, and Windows , pokud je produkt IBM WebSphere MQ Version 7.1nebo novější, knihovny načíteny, produkt IBM WebSphere MQ automaticky použije příslušné knihovny, aniž byste potřebovali provést další akce. IBM WebSphere 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 WebSphere MQ:

propojení
Při kompilování aplikace je aplikace propojena s knihovnami produktu IBM WebSphere MQ , aby získal export funkcí, který se poté načte při spuštění aplikace.

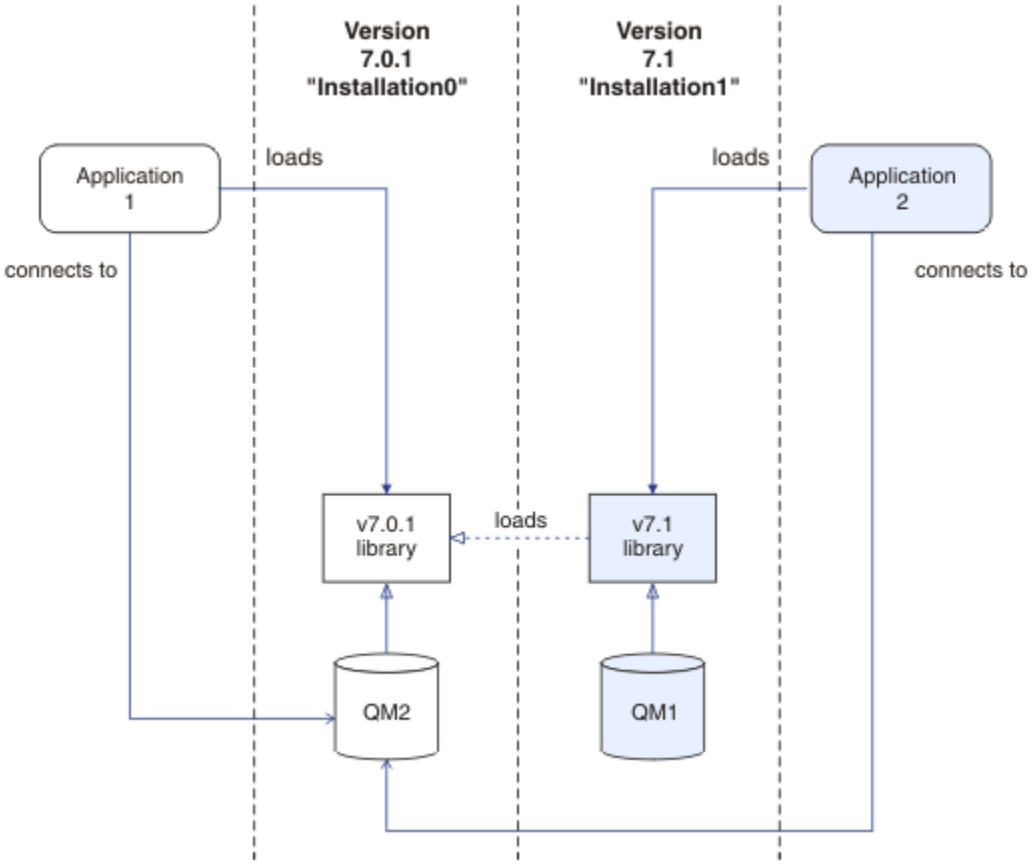
Zavádění
Když je aplikace spuštěna, jsou umístěny a zavedeny knihovny produktu IBM WebSphere MQ . Specifický mechanismus použitý k vyhledání knihoven se liší podle operačního systému a podle toho, jak je aplikace sestavena. Další informace o tom, jak vyhledat a načíst knihovny ve více instalačních prostředích, najdete v tématu “Načtení IBM WebSphere MQ Version 7.1 nebo novějších knihoven” na stránce 8.

Připojování
Když se aplikace připojí ke spuštěnému správci front, například pomocí volání `MQCONN` nebo `MQCONNX` , připojí se k použití načtených knihoven produktu IBM WebSphere 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 mechanizmu, který operační systém používá k vyhledání knihoven produktu IBM WebSphere 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 Version 7.1nebo pozdější knihovny, jsou umístěny a zavedeny, IBM WebSphere MQ pak zavede a použije příslušné knihovny, aniž byste potřebovali provést další akce. Když se aplikace připojí ke správci front, produkt IBM WebSphere MQ načte knihovny z instalace, ke které je přidružen správce front.



Obrázek 1. Připojování aplikací v prostředí s více instalačními prostředí

Například produkt Obrázek 1 na stránce 7 zobrazuje více instalačních prostředí s instalací verze 7.0.1 (`Installation0`) a instalací 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 `QM1`nebo 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 verze produktu 7.0.1 není schopna načíst jiné verze knihovny. To znamená, že pokud jsou knihovny verze 7.0.1 přímo načteny, nemůžete použít správce front přidruženého k instalaci v novější verzi produktu IBM WebSphere MQ.

Produkt `Application 2` přímo načte knihovnu verze 7.1 . Když se produkt `application 2` připojí k produktu `QM2`, knihovna 7.1 se poté načte a použije knihovnu verze 7.0.1 . Pokud se produkt `application 2` připojí k produktu `QM1`nebo pokud je produkt `QM2` přidružen k produktu `Installation1`, načte se knihovna verze 7.1 a aplikace pracuje podle očekávání.

Scénáře migrace a připojení aplikací s více instalacemi jsou podrobněji zvážené v tématu Koexistence více instalačních správců front v systémech UNIX, Linuxa Windows.

Další informace o tom, jak načíst knihovny IBM WebSphere MQ Version 7.1 , viz “Načtení IBM WebSphere MQ Version 7.1 nebo novějších knihoven” na stránce 8.

Podpora a omezení

Pokud jsou některé z následujících verzí 7.1nebo novější knihovny umístěny a načteny, produkt IBM WebSphere MQ může 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 WebSphere 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 naleznete v části "Omezení pro aplikace používající více instalací" na stránce 11.

Související pojmy

"Přidružení správce front k instalaci" na stránce 16
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému UNIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

"Omezení pro aplikace používající více instalací" na stránce 11
Při používání knihoven serveru CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními programy jsou omezení.

"Načtení IBM WebSphere MQ Version 7.1 nebo novějších knihoven" na stránce 8
Při rozhodování o načtení knihoven produktu IBM WebSphere MQ je třeba zvážit řadu faktorů, včetně: vašeho prostředí, zda můžete změnit existující aplikace, zda chcete primární instalaci, kde je nainstalován produkt IBM WebSphere MQ a zda se bude umístění produktu IBM WebSphere MQ pravděpodobně měnit.

Související úlohy

Výběr primární instalace
"Změna primární instalace" na stránce 15
K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz **setmqinst** .

Načtení IBM WebSphere MQ Version 7.1 nebo novějších knihoven

Při rozhodování o načtení knihoven produktu IBM WebSphere MQ je třeba zvážit řadu faktorů, včetně: vašeho prostředí, zda můžete změnit existující aplikace, zda chcete primární instalaci, kde je nainstalován produkt IBM WebSphere MQ a zda se bude umístění produktu IBM WebSphere MQ pravděpodobně měnit.

Způsob umístění a načítání knihoven produktu IBM WebSphere MQ Version 7.1 závisí na vašem instalačním prostředí:

- Je-li v systému UNIX and Linux nainstalována kopie produktu IBM WebSphere MQ Version 7.1 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 verze 7.1 , aby byla primární instalací, nebo ručně vytvořit symbolické odkazy.
- Je-li produkt IBM WebSphere MQ Version 7.1 nainstalován v jiném než výchozím umístění, což je případ, kdy je nainstalován také produkt IBM WebSphere MQ Version 7.0.1 , může být zapotřebí změnit existující aplikace tak, aby byly načteny správné knihovny.

Jak produkt IBM WebSphere MQ Version 7.1nebo pozdější 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 10.

Optimálně byste měli zajistit, aby správce front byl přidružen ke knihovně IBM WebSphere MQ , která je zavedena operačním systémem.

Metody načítání knihoven IBM WebSphere MQ se liší podle platformy a každá z těchto metod má výhody a nevýhody.

Tabulka 1. Výhody a nevýhody voleb pro načítání knihoven

Platforma	Volba	Výhody	Nevýhody
Systémy UNIX and Linux	Nastavte nebo změňte cestu k vestavěné běhové vyhledávací cestě (RPath) aplikace. Tato volba vyžaduje opětovnou kompilaci a propojení aplikace. Další informace o kompilaci a propojování aplikací najdete v tématu Sestavení aplikace WebSphere MQ.	• Rozsah změny je jasný.	• Musíte být schopni znovu zkompilovat a propojit aplikaci. • Změní-li se umístění IBM WebSphere MQ , musíte změnit cestu k RPath.
Systémy UNIX and Linux	Nastavte proměnnou prostředí *LD_LIBRARY_PATH* (*LIBPATH* na AIX) pomocí příkazu setmqenvnebo crtmqenvs volbou **-k** nebo **-1** .	• Nejsou vyžadovány žádné změny v existujících požadovaných aplikacích. • Přepíše vložené cesty RPath v aplikaci. • Snadné změny proměnné, pokud se změní umístění produktu IBM WebSphere MQ .	• Aplikace `setuid` a `setgid` nebo aplikace vytvořené jinými způsoby mohou *LD_LIBRARY_PATH* ignorovat z bezpečnostních důvodů. • Specifické prostředí musí být nastaveno v každém prostředí, kde je spuštěna aplikace. • Možný dopad na jiné aplikace, které spoléhají na *LD_LIBRARY_PATH*. • HP-UX: Volby použité při kompilování aplikace mohou zakázat použití proměnné prostředí *LD_LIBRARY_PATH*. Další informace naleznete v tématu Aspekty propojování běhového prostředí pro systém HP-UX. • Linux: Kompilátor použitý k sestavení aplikace může zakázat použití proměnné prostředí *LD_LIBRARY_PATH*. Další informace naleznete v tématu Pokyny týkající se propojení běhového prostředí pro produkt Linux.

Tabulka 1. Výhody a nevýhody voleb pro načítání knihoven (pokračování)			
Platforma	**Volba**	**Výhody**	**Nevýhody**
Systémy Windows	Nastavte proměnnou PATH pomocí příkazu setmqenvnebo crtmqenv.	• Pro existující aplikace nejsou vyžadovány žádné změny. • Snadné změny proměnné, pokud se změní umístění produktu IBM WebSphere MQ .	• Specifické prostředí musí být nastaveno v každém prostředí, kde je spuštěna aplikace. • Možný dopad na jiné aplikace.
Systémy UNIX, Linux, and Windows	Nastavte primární instalaci na verzi 7.1nebo novější, instalaci. Viz “Změna primární instalace” na stránce 15. Další informace o primární instalaci naleznete v tématu Výběr primární instalace .	• Pro existující aplikace nejsou vyžadovány žádné změny. • Snadné změny primární instalace, pokud se změní umístění produktu IBM WebSphere MQ . • Poskytuje podobné chování jako předchozí verze produktu IBM WebSphere MQ.	• Je-li nainstalován produkt WebSphere MQ verze 7.0.1 , nemůžete nastavit primární instalaci na verzi 7.1nebo novější. • UNIX and Linux: Nefunguje, pokud `/usr/lib` není ve výchozí vyhledávací cestě.

Aspekty implementace knihovny pro produkt HP-UX

Ukázkové kompilační příkazy kompilace v dokumentaci produktu pro předchozí verze produktu IBM WebSphere 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 WebSphere MQ z jiného umístění, než je umístění uvedené v cestě k načtení, musíte aktualizovat aplikace. Aplikace můžete aktualizovat opětovným kompilováním a propojením bez volby propojení `-W1, +noenvvar` , nebo pomocí příkazu **`chatr`** .

Chcete-li zjistit, jak vaše aplikace aktuálně zavádějí knihovny, prohlédněte si téma “Mechanismy zavádění knihoven operačního systému” na stránce 10.

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 WebSphere MQ obsahovaly volby propojení produktu `-lmqmcs -lmqmzse` . Odpovídající verze těchto knihoven jsou nyní načíteny automaticky produktem IBM WebSphere MQ. Pokud je produkt IBM WebSphere MQ nainstalován v jiném než výchozím umístění, nebo pokud v systému existuje více instalací, musíte aktualizovat své aplikace. Aplikace můžete aktualizovat opětovným kompilováním a propojením bez voleb odkazu `-lmqmcs -lmqmzse` .

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 UNIX and 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 jsou prohledány pro vyžadované knihovny produktu WebSphere 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 WebSphere 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 Version 7.1 do výchozího umístění, nebo použít jinou metodu k vyhledání knihoven.
- Použije se výchozí cesta ke knihovně. Pokud se knihovny produktu WebSphere MQ nenaleznou po vyhledání umístění proměnné prostředí *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 mechanizmus 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 16
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému UNIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

“Omezení pro aplikace používající více instalací” na stránce 11
Při používání knihoven serveru CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními programy jsou omezení.

“Připojování aplikací v prostředí s více instalačními prostředí” na stránce 6
Pokud je v systémech UNIX, Linux, and Windows , pokud je produkt IBM WebSphere MQ Version 7.1nebo novější, knihovny načíteny, produkt IBM WebSphere MQ automaticky použije příslušné knihovny, aniž byste potřebovali provést další akce. IBM WebSphere MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Související úlohy

Výběr primární instalace

“Změna primární instalace” na stránce 15
K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz **setmqinst** .

Omezení pro aplikace používající více instalací

Při používání knihoven serveru CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními programy jsou omezení.

Knihovny serveru CICS

Používáte-li knihovny serveru CICS , produkt IBM WebSphere MQ pro vás automaticky nevybere správnou úroveň knihovny. Musíte zkompilovat 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 rutin 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 IBM WebSphere MQ Version 7.1nebo 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 IBM WebSphere MQ a nemohou se odkazovat na knihovny IBM WebSphere MQ . Další informace viz Psaní a kompilace ukončení a instalovatelných služeb.

Rychlý způsob

Na serveru s více instalacemi musí aplikace používající připojení rychlým způsobem k IBM WebSphere MQ Version 7.1 nebo novějšímu splňovat tato pravidla:

1. Správce front musí být přidružen ke stejné instalaci jako ten, ze kterého aplikace načetla běhové knihovny IBM WebSphere MQ. Aplikace nesmí používat připojení rychlým způsobem ke správci front přidruženého k jiné instalaci. Při pokusu o vytvoření připojení dojde k chybě. Kód příčiny: MQRC_INSTALLATION_MISMATCH.
2. Připojení jinak než rychlým způsobem ke správci front přidruženému ke stejné instalaci, ze které aplikace načetla běhové knihovny IBM WebSphere 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 Version 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 Version 7.0.1 s připojením rychlým způsobem ke správci front přidruženému k instalaci Version 7.1 nebo novější.

S nastavenou proměnnou AMQ_SINGLE_INSTALLATION můžete vytvořit jakékoli připojení ke správci front rychlým způsobem připojení. Jinak platí téměř stejná omezení:

- Instalace musí být stejná jako ta, ze které byly načteny běhové knihovny produktu IBM WebSphere MQ.
- Všechna připojení k jednomu procesu musí být ke stejné instalaci. Pokusíte-li se připojit ke správci front přidruženému k jiné instalaci, připojení selže s kódem příčiny MQRC_INSTALLATION_MISMATCH. Všimněte si, že s nastavenou proměnnou AMQ_SINGLE_INSTALLATION platí toto omezení pro všechna připojení, nejen pro připojení rychlým způsobem.
- Připojte pouze jednoho správce front s připojeními rychlým způsobem.

Související odkazy

MQCONNX-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 .NET v prostředí s více instalačními prostředí

Při výchozím nastavení aplikace používají sestavení .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* .

Pokud je v systému primární instalace, jsou soubory sestavení .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 sestav .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 verzí produktu IBM WebSphere MQ než verze, se kterou byla aplikace kompilována.

Informace o tom, jak aktualizovat konfigurační soubor aplikace, viz "Připojení aplikací .NET pomocí konfiguračního souboru aplikace" na stránce 13.

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 neprimární instalace.

Další informace o tom, jak aktualizovat proměnnou *DEVPATH* naleznete v tématu "Připojení aplikací .NET pomocí DEVPATH" na stránce 14.

Připojení aplikací .NET pomocí 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 aplikace, aby se aplikace .NET připojily pomocí konkrétních sestav:

Tabulka 2. Konfigurace aplikací pro použití konkrétních sestav

	Aplikace kompilované s nižší verzí produktu IBM WebSphere MQ	**Aplikace kompilované s vyšší verzí produktu IBM WebSphere MQ**
Chcete-li spustit aplikaci s primární instalací produktu IBM WebSphere MQ s vyšší verzí. (sestavy s vyšší verzí v GAC):	Nejsou nutné žádné změny	Nejsou nutné žádné změny
Chcete-li spustit aplikaci s primární instalací produktu IBM WebSphere MQ nižší verze. (dolní sestavy verzí v GAC):	Nejsou nutné žádné změny	V konfiguračním souboru aplikace: • Použijte značku *<bindingRedirect>* k označení použití nižší verze sestav, které jsou v GAC.

Tabulka 2. Konfigurace aplikací pro použití konkrétních sestav (pokračování)		
	Aplikace kompilované s nižší verzí produktu IBM WebSphere MQ	**Aplikace kompilované s vyšší verzí produktu IBM WebSphere MQ**
Chcete-li spustit aplikaci s vyšší verzí produktu IBM WebSphere MQ , než je primární instalace. (sestavy s vyšší verzí v instalační složce):	V konfiguračním souboru aplikace: • Použijte značku *< codebase>* k umístění do umístění sestav s vyšší verzí • Značku *<bindingRedirect>* použijte k označení použití sestav s vyšší verzí.	V konfiguračním souboru aplikace: • Použijte značku *< codebase>* k umístění do umístění sestav s vyšší verzí
Chcete-li spustit aplikaci s nižší verzí produktu IBM WebSphere MQ , která není primární instalací. (sestavy s nižší verzí v instalační složce):	V konfiguračním souboru aplikace: • Použijte značku *< codebase>* k určení umístění sestav s nižší verzí • Zahrnout značku *< publisherpolicy Apply=no>*	V konfiguračním souboru aplikace: • Použijte značku *< codebase>* k určení umístění sestav s nižší verzí • Značku *<bindingRedirect>* použijte k označení použití sestav s nižší verzí • Zahrnout značku *< publisherpolicy Apply=no>*

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 WebSphere 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 používat tuto proměnnou, najdete v příslušné dokumentaci Microsoft *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 6
Pokud je v systémech UNIX, Linux, and Windows , pokud je produkt IBM WebSphere MQ Version 7.1nebo novější, knihovny načíteny, produkt IBM WebSphere MQ automaticky použije příslušné knihovny, aniž byste potřebovali provést další akce. IBM WebSphere MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Více instalací

Související úlohy
Výběr primární instalace
Použití .NET

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 UNIX, Linux, and Windows.

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 Version 7.1 nebo novější koexistující s instalací produktu IBM WebSphere MQ Version 7.0.1, instalace produktu IBM WebSphere MQ Version 7.0.1 musí být primární. Je označen jako primární, je-li nainstalována verze produktu IBM WebSphere MQ Version 7.1 nebo vyšší, a instalaci produktu IBM WebSphere MQ Version 7.1 nebo novější nelze provést jako primární.

Během procesu instalace v systému Windowsmůžete určit, že se má instalace primární instalací. Na systémech UNIX and Linux musíte po instalaci zadat příkaz **setmqinst** , který nastaví instalaci jako primární instalaci.

“Nastavit primární instalaci” na stránce 15.

“Zrušit nastavení primární instalace” na stránce 16.

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 Version 7.1 nebo pozdější.
2. Je-li existující instalace produktu IBM WebSphere MQ Version 7.1 nebo novější nastavena jako primární instalace, zrušte její nastavení podle pokynů uvedených v tématu “Zrušit nastavení primární instalace” na stránce 16. Je-li v systému nainstalován produkt IBM WebSphere MQ Version 7.0.1 , nelze primární instalaci změnit.
3. Jako uživatel root v systémech UNIX and Linux nebo člen skupiny administrátorů 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 Version 7.1 nebo pozdější.

   Je-li produkt IBM WebSphere MQ Version 7.0.1 primární instalací, nemůžete zrušit nastavení primární instalace.
2. Jako uživatel root v systémech UNIX and Linux nebo člen skupiny administrátorů 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 pojmy

Funkce, které lze použít pouze s primární instalací v systému Windows

Odkazy na externí knihovny a řídicí příkazy pro primární instalaci na systému UNIX a Linux

Související úlohy

Odinstalování, upgrade a údržba primární instalace

Výběr názvu instalace

Související odkazy

setmqinst

Přidružení správce front k instalaci

Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému UNIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

Příkaz **setmqm** lze použít následujícími způsoby:

- Přesun jednotlivých správců front mezi obdobnými verzemi produktu WebSphere MQ. Například přesun správce front z testovacího do produkčního systému.
- Migrace jednotlivých správců front ze starší verze produktu WebSphere MQ na novější verzi produktu WebSphere 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 WebSphere 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 nainstalován produkt 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** . 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 přidruženi k odstraněným instalacím

Je-li instalace, ke které je přidružen správce front, odstraněna, nebo pokud jsou informace o stavu správce front nedostupné, příkaz **setmqm** nepřidružuje 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 mqs.ini tak, aby určoval jinou instalaci.
3. K odstranění správce front použijte příkaz **dltmqm** z této instalace.

Související pojmy

“Vyhledání instalací produktu IBM WebSphere MQ v systému” na stránce 17
Máte-li v systému více instalací produktu IBM WebSphere MQ , můžete zkontrolovat, které verze jsou nainstalované a kde jsou.

“Konfigurační soubor IBM WebSphere MQ , mqs.ini .” na stránce 408
Konfigurační soubor IBM WebSphere MQ mqs.iniobsahuje informace vztahující se ke všem správcům front v daném uzlu. Vytvoří se automaticky během instalace.

Související úlohy

Výběr primární instalace

Související odkazy

setmqm

strmqm

dspmq

dspmqinst

Vyhledání instalací produktu IBM WebSphere MQ v systému

Máte-li v systému více instalací produktu IBM WebSphere MQ , můžete zkontrolovat, které verze jsou nainstalované a kde jsou.

K vyhledání instalací produktu IBM WebSphere 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 Version 7.0.1 .
- Použijte instalační nástroje platformy pro dotaz, kde byl nainstalován produkt IBM WebSphere MQ . Potom použijte příkaz **dspmqver** z instalace produktu Version 7.1 nebo novější. Následující příkazy jsou příklady příkazů, které můžete použít k dotazování tam, kde byl nainstalován produkt IBM WebSphere 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 balíků 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 UNIX and Linux zadejte následující příkaz, abyste zjistili, kde je nainstalován produkt IBM WebSphere MQ :

  ```
  cat /etc/opt/mqm/mqinst.ini
  ```

  Potom použijte příkaz **dspmqver** z instalace produktu Version 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 Version 7.1 nebo pozdější.

Související pojmy
Více instalací
Související odkazy
dspmqver
dspmqinst

Vytváření a údržba správců front

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 služby systému front aplikacím pro rozhraní MQI (Message Queuing Interface) a příkazy k vytvoření, úpravě, zobrazení a odstranění objektů produktu IBM WebSphere MQ .

Chcete-li vytvořit správce front, použijte řídicí příkaz IBM WebSphere 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 WebSphere MQ nepodporuje názvy počítačů, které obsahují mezery. Pokud instalujete produkt IBM WebSphere MQ na počítač s názvem počítače, který obsahuje mezery, nemůžete vytvořit žádné správce front.

Zapnuto

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 systému Windows nepřidá uživatele, který provádí instalaci do skupiny mqm, další podrobnosti viz Oprávnění ke správě IBM WebSphere MQ v systémech UNIX, Linux a Windows.

Konvence pojmenování
V názvech používejte velká písmena, aby byla možná komunikace se správci 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.

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 WebSphere MQ pro komunikaci s jinými podniky, můžete také jako předponu zahrnout také vlastní podnikový název. To se v příkladech nedějí, protože je ztížit 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 WebSphere MQ na uzlu bez jednoho. Výchozí správce front je správce front, ke kterému se aplikace připojují, pokud ve volání MQCONN neurčují 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 směrována 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 21.

Určit frontu nedoručených zpráv

Fronta nedoručených zpráv je lokální fronta, do které jsou odesílány zprávy, pokud je nelze směrovat 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 pomocí 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 300.

Pouze pro systémy IBM WebSphere MQ pro systémy 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" 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 23
Konfigurační informace produktu IBM WebSphere MQ jsou uloženy v konfiguračních souborech v systémech Windows, UNIX and Linux .

"Spuštění správce front" na stránce 24
Při vytváření správce front je nutné jej spustit, aby bylo možné ji povolit pro zpracování příkazů nebo volání MQI.

"Zastavení správce front" na stránce 24
Existují tři způsoby, jak zastavit správce front: klidové ukončení a okamžité ukončení práce systému a preventivní ukončení práce.

"Restartování správce front" na stránce 25
Pomocí příkazu **strmqm** lze restartovat správce front nebo v systémech IBM WebSphere MQ for Windows a IBM WebSphere MQ for Linux (platformyx86 a x86-64) restartovat správce front z produktu IBM WebSphere MQ Explorer.

"Změna konfiguračních informací IBM WebSphere MQ a správce front" na stránce 406
Změňte chování produktu IBM WebSphere MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Systémové a výchozí objekty

Související úlohy

"Nastavení výchozího správce front jako výchozího správce front" na stránce 22
Můžete vytvořit existujícího správce front jako výchozího správce front. Způsob, jakým to provedete, závisí na použité platformě.

"Odstranění správce front" na stránce 26
Správce front můžete odstranit pomocí příkazu **dltmqm** nebo pomocí Průzkumníka produktu WebSphere MQ .

distributed 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 WebSphere MQ **crtmqm**.

Než začnete

Před vytvořením výchozího správce front si přečtěte informace popsané v tématu "Vytváření a údržba správců front" na stránce 18.

UNIX Pokud k vytvoření správce front v produktu UNIX and Linuxpoužíváte 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 Windowsmůžete 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 WebSphere 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 WebSphere 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 **strmqm** ke spuštění správce front.

Související pojmy

“Zálohování konfiguračních souborů po vytvoření správce front” na stránce 23
Konfigurační informace produktu IBM WebSphere MQ jsou uloženy v konfiguračních souborech v systémech Windows, UNIX and Linux .

Práce se správci front

Práce s lokálními frontami

Související odkazy

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.

Systémy WebSphere MQ for Windows a WebSphere MQ for Linux (platformyx86 a x86-64)

Informace o této úloze

Chcete-li vytvořit existujícího správce front jako výchozího správce front v produktu WebSphere MQ for Windows a WebSphere MQ for Linux (platformyx86 a x86-64), postupujte podle následujících pokynů:

Postup

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

Systémy UNIX and Linux

Informace o této úloze

Při vytváření výchozího správce front je jeho název vložen do atributu `Name` oddílu `DefaultQueueManager` v konfiguračním souboru produktu WebSphere 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 WebSphere MQ a správce front” na stránce 406 .

Zálohování konfiguračních souborů po vytvoření správce front

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

V systémech Windows a Linux (x86 a x86-64) používají systémy IBM WebSphere 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 WebSphere 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.

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 WebSphere MQ a správce front" na stránce 406.

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 `dspmq -o installation` můžete zjistit, která instalace správce front je přidružena.

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

```
strmqm QMB
```

Na systémech WebSphere MQ for Windows a WebSphere MQ for Linux (platformyx86 a x86-64) můžete spustit správce front následujícím způsobem:

1. Otevřete Průzkumníka IBM WebSphere 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 WebSphere MQ vydá 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 WebSphere MQ for Windows můžete spustit správce front automaticky, když se systém spustí pomocí Průzkumníka IBM WebSphere MQ . Další informace najdete v tématu Administrace pomocí produktu IBM WebSphere 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 `dspmq -o installation` můžete zjistit, která instalace správce front je přidružena.

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

```
endmqm QMB
```

Na systémech WebSphere MQ for Windows a WebSphere MQ for Linux (platformyx86 a x86-64) můžete správce front zastavit následujícím způsobem:

1. Otevřete Průzkumníka IBM WebSphere 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:

- Nezaškrtli 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 restartovat správce front nebo v systémech IBM WebSphere MQ for Windows a IBM WebSphere MQ for Linux (platformyx86 a x86-64) restartovat správce front z produktu IBM WebSphere MQ Explorer.

Chcete-li restartovat správce front, zadejte příkaz:

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

V systémech IBM WebSphere MQ for Windows a IBM WebSphere MQ pro systémy Linux (platformyx86 a x86-64) můžete správce front restartovat stejným způsobem jako jeho spuštění, a to následujícím způsobem:

1. Otevřete Průzkumníka IBM WebSphere 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, produkt IBM WebSphere MQ odešle informační zprávy přerušovaně podrobně popisující průběh spouštění.

Odstranění správce front

Správce front můžete odstranit pomocí příkazu **dltmqm** nebo pomocí Průzkumníka produktu WebSphere 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 `dspmq -o installation` můžete zjistit, která instalace správce front je přidružena.

Postup odstranění správce front

Informace o této úloze

V systémech WebSphere MQ for Okna a WebSphere MQ for Linux (v platformáchx86 a x86-64) můžete správce front odstranit následujícím způsobem:

Postup

1. Otevřete produkt WebSphere MQ Explorer.
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 odstraníte 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 měnit svou mysl; když stisknete klávesu Enter, všechny přidružené prostředky se ztratí.
- Při odstraňování správce front v produktu WebSphere MQ for Windowssprávce front také odebere správce front ze seznamu automatického spouštění (viz popis v tématu “Spuštění

správce front” na stránce 24). Po dokončení příkazu se zobrazí zpráva `WebSphere 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 systému Windows, UNIX and Linux systémy .)

Připojování aplikací pomocí distribuovaných front

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu WebSphere 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 Koncepce vzájemné komunikace .

Informace v následujících odkazech použijte k připojení aplikací pomocí distribuovaných front:

- “Jak odeslat zprávu jinému správci front” na stránce 49
- “Spouštěcí kanály” na stránce 66
- “Bezpečnost zpráv” na stránce 64
- “Techniky distribuovaného systému zpráv produktu IBM WebSphere MQ” na stránce 27
- “Úvod do distribuované správy front” na stránce 46
- Windows Linux UNIX “Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 72

Související pojmy

“Konfigurace připojení mezi klientem a serverem” na stránce 96
Chcete-li konfigurovat komunikační spojení mezi klienty a servery produktu WebSphere MQ MQI, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích propojení, spusťte modul listener a definujte kanály.

“Změna konfiguračních informací IBM WebSphere MQ a správce front” na stránce 406
Změňte chování produktu IBM WebSphere MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související úlohy

“Konfigurace klastru správce front” na stránce 156
Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

Techniky distribuovaného systému zpráv produktu IBM WebSphere MQ

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

Související pojmy

“Připojování aplikací pomocí distribuovaných front” na stránce 27
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu WebSphere MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Kanály
Úvod do systému front zpráv
Koncepce interkomunikace

Související odkazy
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 “Připojování aplikací pomocí distribuovaných front” na stránce 27. Je-li správce front v klastru, je tok zpráv řízen pomocí různých technik, jak je popsáno v tématu “řízení toku zpráv” na stránce 28.

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 Objekty . 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 okapovat o konceptech rozlišení názvu a o třech způsobech použití definic vzdálených front. Viz Concepts of intercommunication.

Související pojmy
“Názvy front v záhlaví přenosu” na stránce 28
Názvy cílových front cestují se zprávou v záhlaví přenosu, dokud není dosažena cílová fronta.

“Jak vytvořit správce front a odpovědět na aliasy” na stránce 29
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-služby.

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. Tabulka 3 na stránce 29 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 3. Tři způsoby použití objektu definice vzdálené fronty

Pouľití	**Název správce front**	**Název fronty**	**Jméno přenosové fronty**
1. Definice vzdálené fronty (při volání OPEN)			
Dodáno v rámci volání	prázdné nebo lokální QM	(*) vyžadováno	-
Dodáno v definici	povinné	povinné	volitelné
2. Alias správce front (při volání OPEN)			
Dodáno v rámci volání	(*) požadováno a nikoli lokální QM	povinné	-
Dodáno v definici	povinné	prázdná	volitelné
3. Alias fronty pro odpověď (ve volání PUT)			
Dodáno v rámci volání	prázdná	(*) vyžadováno	-
Dodáno v definici	volitelné	volitelné	prázdná
Poznámka: (*) znamená, že tento název je název objektu definice			

Formální popis naleznete v tématu Rozpoznání názvu fronty.

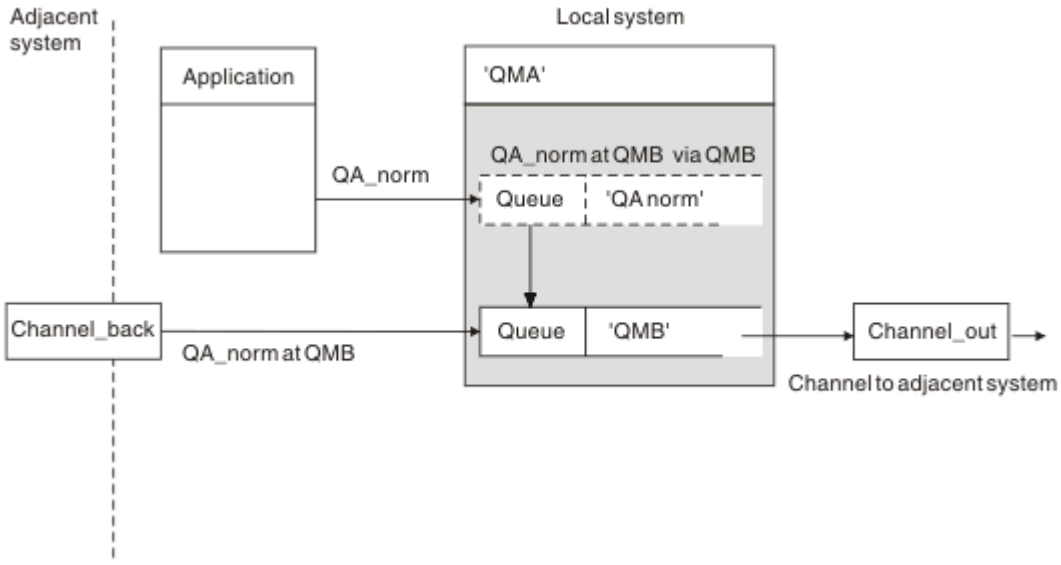
Vložení zpráv do vzdálených front

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 2 na stránce 30 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 2. Definice vzdálené fronty se používá k převedení názvu fronty na přenosovou frontu do sousedního správce front.

Jste-li administrátorem systému WebSphere 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. Další informace najdete v tématu Klastry .

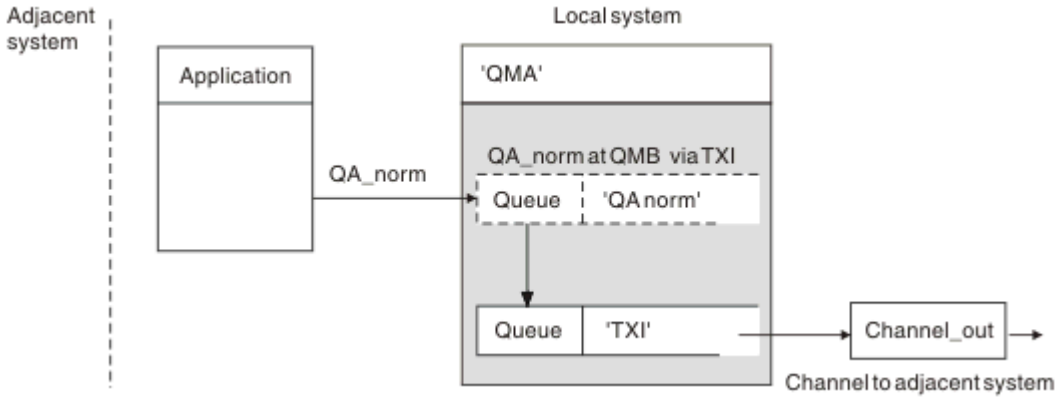
Další informace o rozlišování názvů

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 3. Definice vzdálené fronty umožňuje použití jiné přenosové fronty.

Když v prostředí rozděleném do front potřebujete změnit tok zpráv z jednoho kanálu do jiného, použijte stejnou konfiguraci systému, jak ukazuje Obrázek 2 na stránce 30 v produktu "Vložení zpráv do vzdálených front" na stránce 30. Obrázek 3 na stránce 31 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, kterou uvádí Obrázek 3 na stránce 31, 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.

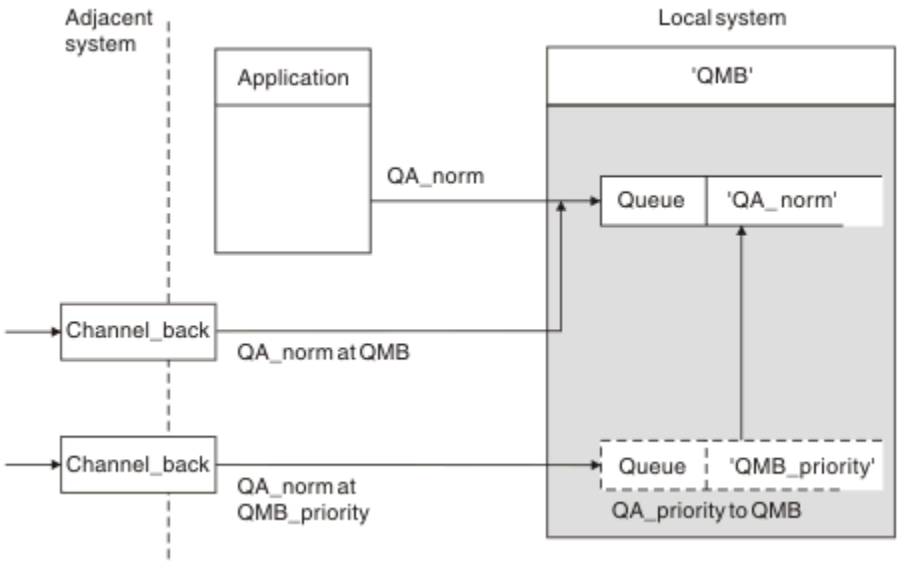
Zprávy jsou umístěny do přenosové fronty 'TX1' s hlavičkou přenosu obsahujícím 'QA_norm při QMB_priority' a jsou posílána přes kanál na sousední systém.

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 naleznete v části "Fronty klastru" na stránce 162.

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 4. 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 4 na stránce 32 .

Pro tuto konfiguraci musíte připravit:

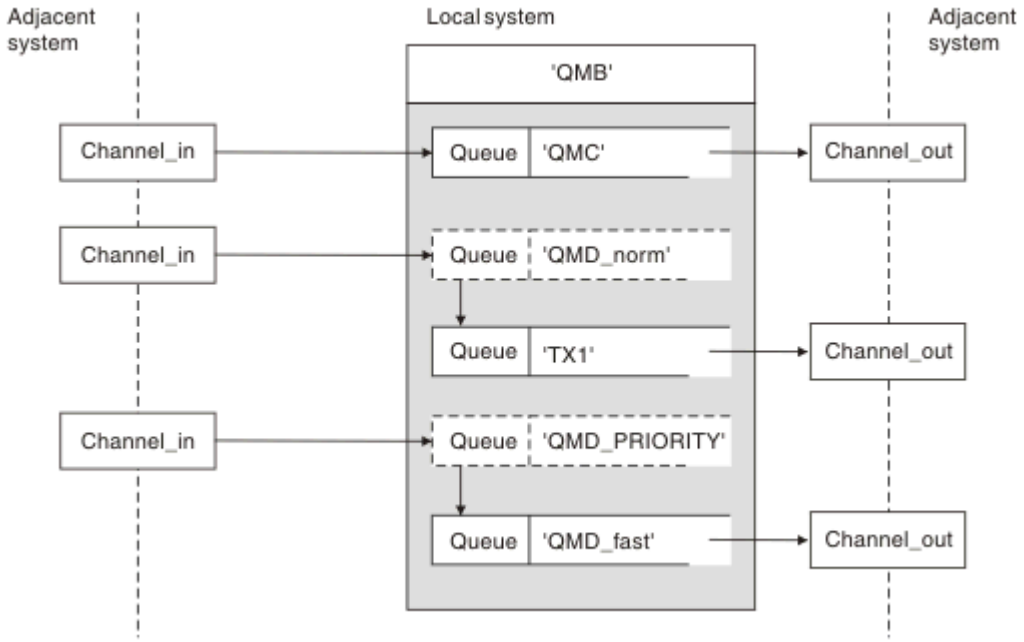
- Kanály zpráv pro příjem zpráv ze sousedních správců front
- Definice aliasu správce front k vyřešení příchozího toku zpráv, 'QMB_priority', do lokálního názvu správce front, 'QMB'
- Lokální fronta, 'QA_norm', pokud neexistuje,

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 5. Tři metody posílání zpráv přes váš systém

Technika zobrazená v Obrázek 4 na stránce 32 v produktu “Příjem zpráv” na stránce 31ukázala, jak je zachycen tok alias. Obrázek 5 na stránce 33 ilustruje způsob, jakým jsou sítě vybudovány tím, že se spojí techniky dříve popsané.

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_norm 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.QUEUEpřenáší 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.

Použít tyto metody

Pro tyto konfigurace musíte připravit:

- Definice vstupního kanálu
- Definice výstupního kanálu
- Přenosové fronty:
  - QMC
  - TX1
  - QMD_fast
- Definice aliasů správce front:

- QMD_norm with QMD_norm 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: Použít 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: Použít 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_norm, tj. pojmenované třídy služby QMD_norm.
- Změní záhlaví přenosu na těchto zprávách z QMD_norm na QMD.

Metoda 3: Vyberte přenosovou frontu

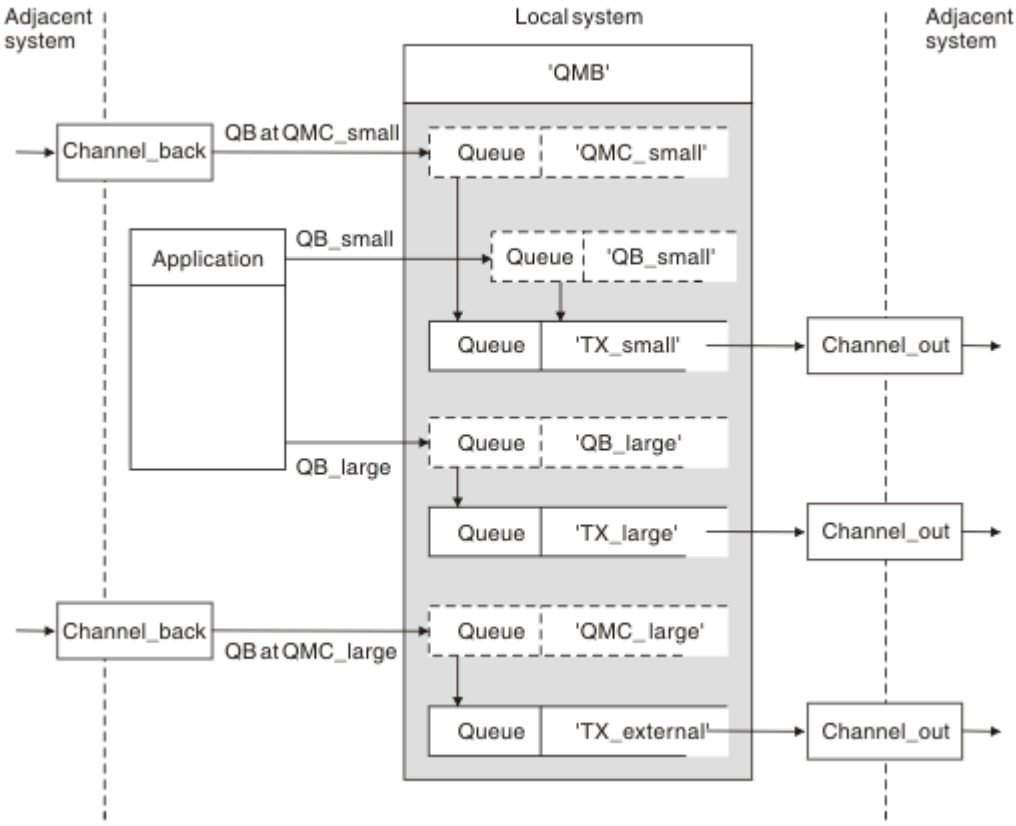
Třetí metodou je alias objektu správce front definovaný se stejným názvem jako cílové umístění, QMD_PRIORITY. Definice aliasu správce front slouží k výběru konkrétní přenosové fronty, produktu QMD_fast, a tedy jiného kanálu. Hlavičky přenosu na těchto zprávách zůstanou nezměněny.

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 směrovat 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 6. Oddělení toků zpráv

V příkladu uvedeném v souboru Obrázek 6 na stránce 35jsou 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 specifikujte 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:

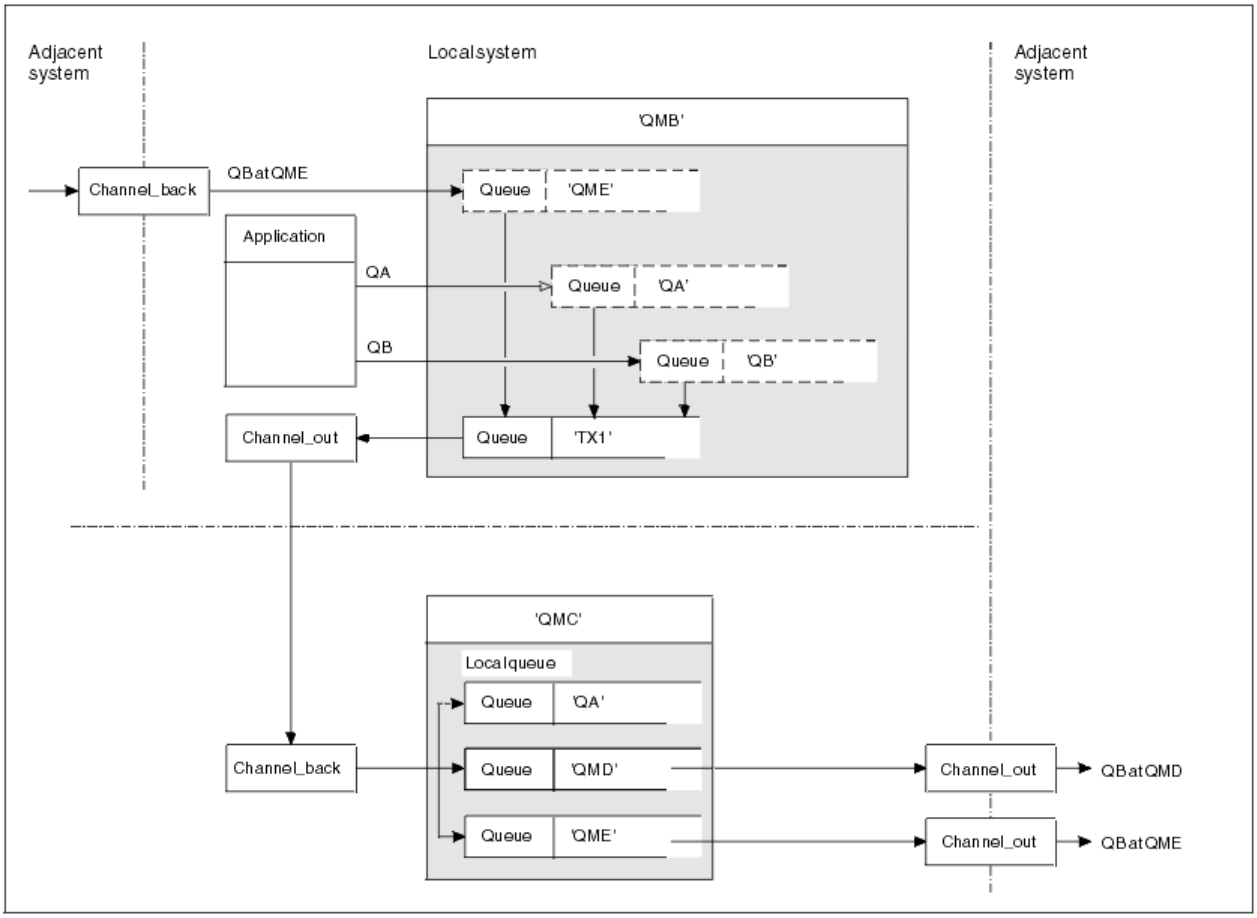
- Definice příchozího kanálu
- Dvě definice vzdálených front QB_small a QB_large
- Dva definice aliasů správce front QMC_small a QMC_large
- Tři definice odesílajícího kanálu
- Tři přenosové fronty: TX_small, TX_large, a TX_external

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 7. Sloučení toků zpráv na kanál

Obrázek 7 na stránce 36 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 určení. 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'

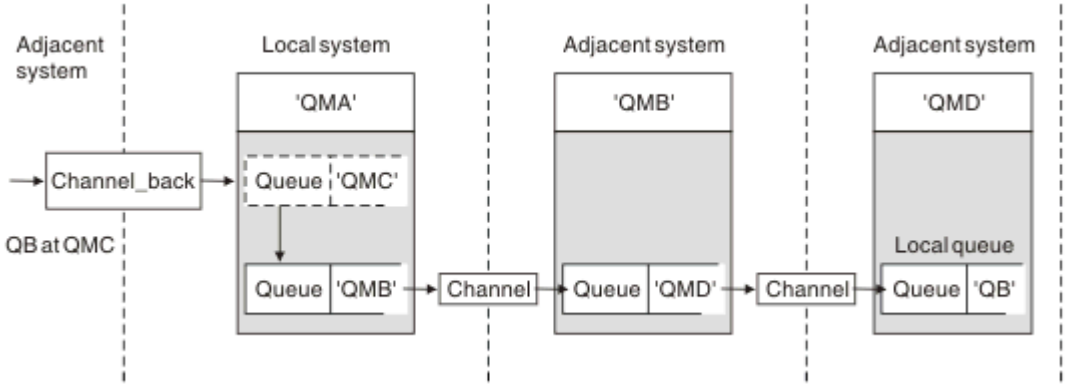
Doplňkový administrátor, který konfiguruje QMC, musí poskytovat:

- 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 8. Odklonění proudů zpráv do jiného cíle

Obrázek 8 na stránce 37 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 opětného 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.

Aliasy lze používat v klastrovém prostředí. Informace viz “Aliasy správce front a klastry” na stránce 252.

Odesílání zpráv do rozdělovníku

Chcete-li aplikaci odeslat zprávu do několika míst určení, můžete použít jediné volání MQPUT.

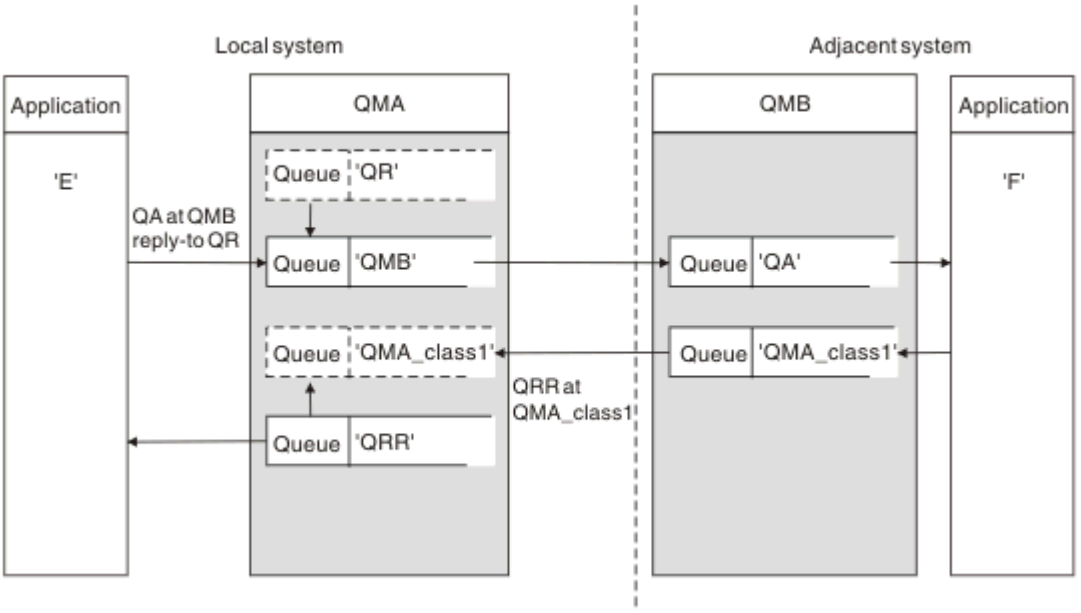
V produktu WebSphere MQ na všech platformách s výjimkou produktu z/OSmůže aplikace odeslat zprávu do několika cílů s jedním voláním MQPUT. Můžete to provést jak v prostředí rozděleném do front, tak i v prostředí klastrů. Musíte definovat cíle v rozdělovníku, jak je popsáno v tématu Distribuční seznamy.

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 9. Substituce názvu fronty pro odpověď během volání PUT

V produktu Obrázek 9 na stránce 38se 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 7 na stránce 45.

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 poskytujete službu pro výběr třídy služeb pro zprávy odpovědí. 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 29
Toto téma vysvětluje tři způsoby, jak můžete vytvořit definici vzdálené fronty.

“Příklad alias fronty pro odpověď” na stránce 39
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.

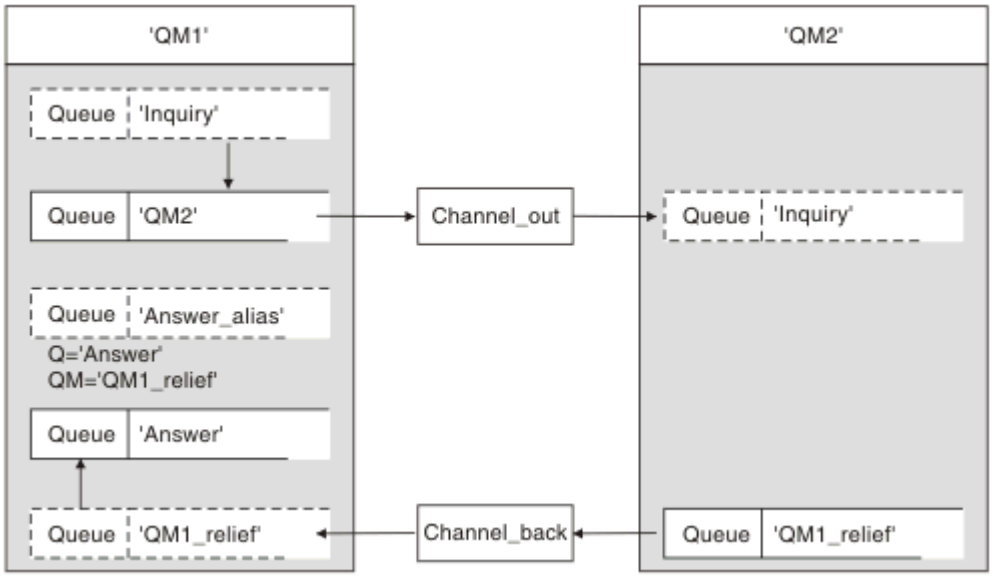
“Jak příklad funguje” na stránce 41
Vysvětlení příkladu a způsobu, jakým správce front používá alias fronty pro odpověď.

“Průchodná odpověď na alias fronty pro odpověď” na stránce 42
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 10 na stránce 40, zpáteční cesta musí být k dispozici pro zprávy odpovědi včetně alias přenosové fronty, kanálu a aliasu správce front.



Obrázek 10. 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 odpovědí '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 odpovědí žadateli na QM1.

Definice použité v tomto příkladu na QM1

Administrátor systému WebSphere MQ na serveru QM1 musí zajistit, aby byla vytvořena odpověď-do fronty 'Odpověď' 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 WebSphere MQ na serveru QM2 musí zajistit, aby lokální fronta pro příchozí zprávy existovala 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 odpovědí a návratové cesty 'QM1_relief'.

Změna názvu fronty 'Answer' je obvykle neužitečná, protože aplikace QM1 očekávají své odpovědi v této frontě. Administrátor systému QM1 však může podle potřeby změnit návratovou trasu (třídu služeb).

Jak správce front používá alias fronty odpovědí 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.

Tabulka 4. Alias fronty pro odpověď

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 frontQM1_reliefje 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 přenese 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 příslušných tématech v sekci Jak klastry fungují v dokumentaci produktu.

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 směrování

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 směrován, se liší od způsobu, jakým je směrována 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 části Tabulka 5 na stránce 44, Tabulka 6 na stránce 44a Tabulka 7 na stránce 45.

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.

Tabulka 5. Rozlišení názvů front ve správci front QMA

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

Tabulka 6. Rozlišení názvů front ve správci front QMB

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

Tabulka 6. Rozlišení názvů front ve správci front QMB (pokračování)

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	QMC	QA	QMC	TX1	Vzdálená fronta
QB	QMD	QB	QMD	TX1	Vzdálená fronta

Tabulka 7. Převod názvu fronty odpovědí na název fronty správce front QMA

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 pro ujištění, že jsou zprávy doručovány, doručovány bez duplikace a uloženy ve stejném pořadí, v jakém byly převzaty z přenosové fronty.

Pořadové číslo je generováno na odesílajícím konci kanálu a je inkrementováno jedním před použitím, což znamená, že aktuální pořadové číslo je číslo poslední odeslané zprávy. Tyto informace lze zobrazit pomocí příkazu DISPLAY CHSTATUS (viz Odkaz na MQSC). Pořadové číslo a identifikátor nazývaný LUWID jsou uloženy v trvalém úložišti pro poslední zprávu přenesenou v dávce. Tyto hodnoty se používají během spouštění 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 získaovány 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.

Na systémech 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 WebSphere 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 přenosových frontách, identifikátorům komunikačního propojení a atributech 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 odesilatele, druhý konec příjemce.

Podrobnosti o tom, jak definovat kanály, najdete v tématu:

- Windows Linux UNIX “Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 72

Příklady plánování kanálů zpráv viz:

- Windows Linux UNIX Příklad plánování kanálů zpráv pro distribuované platformy

Informace o uživatelských procedurách kanálů naleznete v tématu Programy výstupních programů kanálů pro kanály systému zpráv.

Související pojmy

“Odeslání a příjem zprávy” na stránce 47
Následující obrázek ukazuje model distribuované správy front s podrobnými informacemi o vztazích mezi entitami při přenosu zpráv. Zobrazuje také tok pro řízení.

“Řídicí funkce kanálu” na stránce 52
Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

“Co se stane, když nebude možné zprávu doručit?” na stránce 64
Nelze-li zprávu doručit, může ji agent MCA zpracovat několika způsoby. Může to zkusit znovu, může vrátit odesilateli, nebo to může dát do fronty nedoručených zpráv.

“Inicializační a konfigurační soubory” na stránce 68
Zpracování inicializačních dat kanálu závisí na použité platformě WebSphere MQ .

“Převod dat pro zprávy” na stránce 69
Zprávy produktu WebSphere MQ mohou vyžadovat převod dat při odesílání mezi frontami v různých správcích front.

“Psaní vlastních agentů kanálů zpráv” na stránce 70
Produkt WebSphere MQ umožňuje psát vlastní programy MCA (Message Channel Agent) nebo instalovat jeden z nezávislých dodavatelů softwaru.

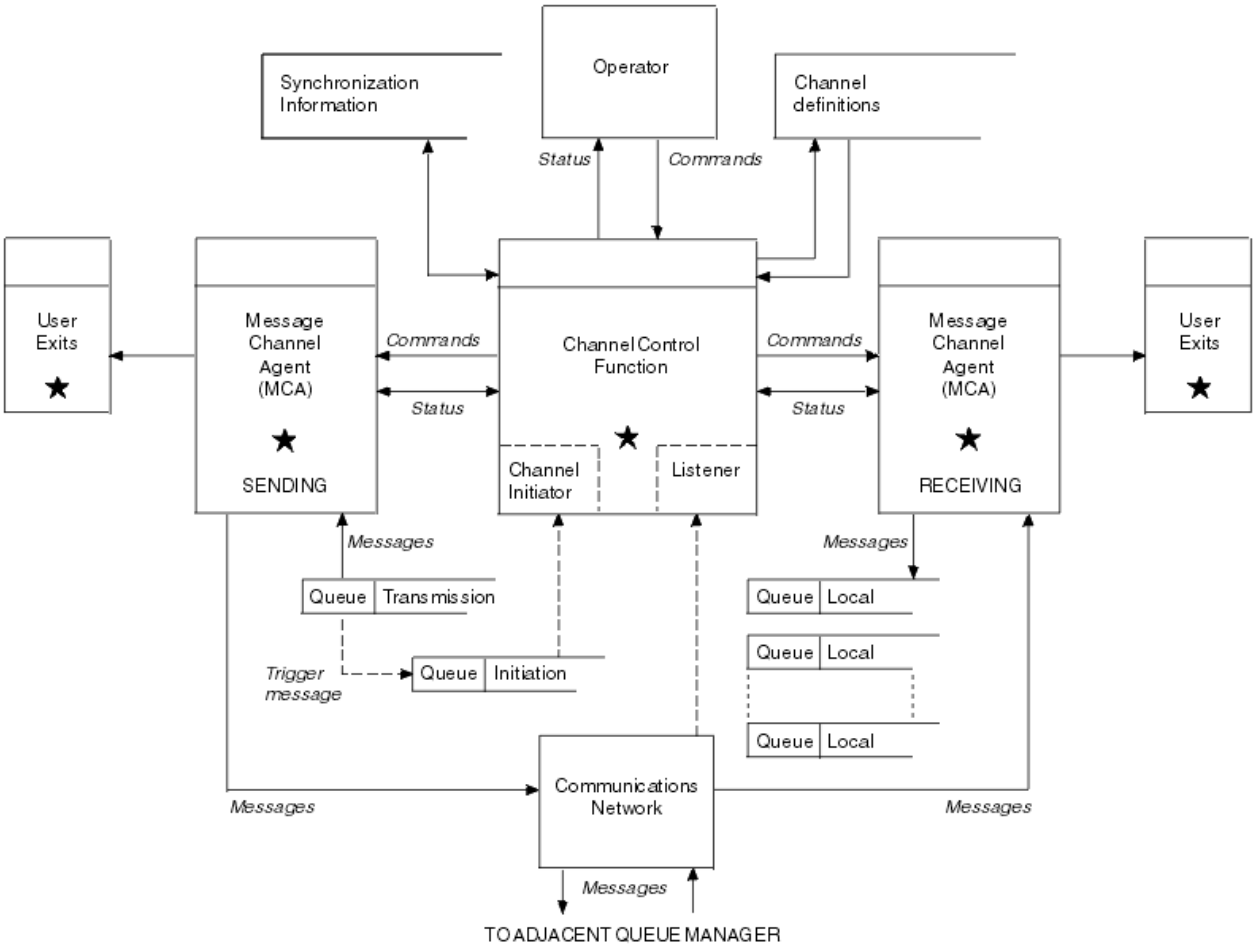
“Další informace, které je třeba zvážit při správě distribuovaných front” na stránce 70
Další témata, která je třeba vzít v úvahu při přípravě produktu WebSphere MQ pro distribuovanou správu front. Toto téma pokrývá frontu nedoručených zpráv, Fronty v použití, Rozšíření systému a programy uživatelských procedur a Spouštění kanálů a listenerů jako ověřené aplikace.

Související odkazy

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 11. 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 odesilatelem, 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 WebSphere 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 (volitelné)
  - Přenosová fronta
  - Fronta nedoručených zpráv
- Definujte následující objekty v cílovém správci front:
  - Kanál příjemce
  - Cílová fronta
  - Fronta nedoručených zpráv

K definování těchto objektů v závislosti na platformě WebSphere MQ můžete použít několik různých metod:

- Na všech platformách můžete použít příkazy skriptu WebSphere MQ (MQSC) popsané v Příkazy MQSC programu pro programovatelné formáty příkazů (PCF) popsané v publikaci Automatizace administračních úloh nebo v Průzkumníku WebSphere MQ .

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 stránce 18

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

“Techniky distribuovaného systému zpráv produktu IBM WebSphere MQ” na stránce 27
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 46
Distribuovaná správa front (DQM) se používá k definování a řízení komunikace mezi správci front.

“Spouštěcí kanály” na stránce 66
Produkt WebSphere MQ poskytuje službu pro automatické spouštění aplikace, jsou-li splněny určité podmínky ve frontě. Toto zařízení se nazývá spouštění.

“Bezpečnost zpráv” na stránce 64
Kromě typických funkcí zotavení produktu WebSphere 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.

“Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 72
Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, IBM WebSphere MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro informace o synchronizaci.

“Konfigurace připojení mezi klientem a serverem” na stránce 96
Chcete-li konfigurovat komunikační spojení mezi klienty a servery produktu WebSphere MQ MQI, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích propojení, spusťte modul listener a definujte kanály.

Související úlohy

“Konfigurace klastru správce front” na stránce 156
Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

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 produktu WebSphere MQ for z/OSmusí 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.

Uveďte jméno komunikačního protokolu, který používáte (atribut TRPTYPE). V produktu WebSphere MQ for z/OSmusí 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.

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.

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.

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

  Nezbytné pro systémy z/OSa volitelné na jiných platformách. Zvažte pojmenování inicializační fronty SYSTEM.CHANNEL.INITQ. na jiných platformách.

- Definice přenosové fronty

  Lokální fronta s atributem USAGE nastaveným na XMITQ.

- 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 51
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

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 příkazy WebSphere MQ Commands (MQSC), jak je uvedeno v následujících příkladech:

Příklad příkazu pro vytvoření přenosové fronty

```
DEFINE QLOCAL(QM2) DESCR('Transmission queue to QM2') USAGE(XMITQ)
```

Příklad příkazu pro vytvoření vzdálené fronty

```
DEFINE QREMOTE(PAYROLL) DESCR('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.

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 *pipeling* 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 WebSphere MQ (MQSC) a řídicí příkazy, které jsou podrobně popsány v produktu “Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 72, 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 WebSphere MQ na všech platformách s výjimkou produktu z/OSneexistuje žádná vhodná 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.RECEIVERnebo SYSTEM.AUTO.SVRCONN. Definice modelových kanálů pro automatickou definici jsou stejné jako výchozí nastavení systému, SYSTEM.DEF.RECEIVERa 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 mezerových 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 WebSphere MQ , jako jsou definice vzdálených front, definice aliasů správce front a definice alias fronty pro odpověď na fronty k implementaci scénářů popsaných v tématu “Připojování aplikací pomocí distribuovaných front” na stránce 27.

Informace o definování kanálů MQI viz “Definování kanálů MQI” na stránce 109.

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 62.

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 odesilatelem, odesilatelem 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).

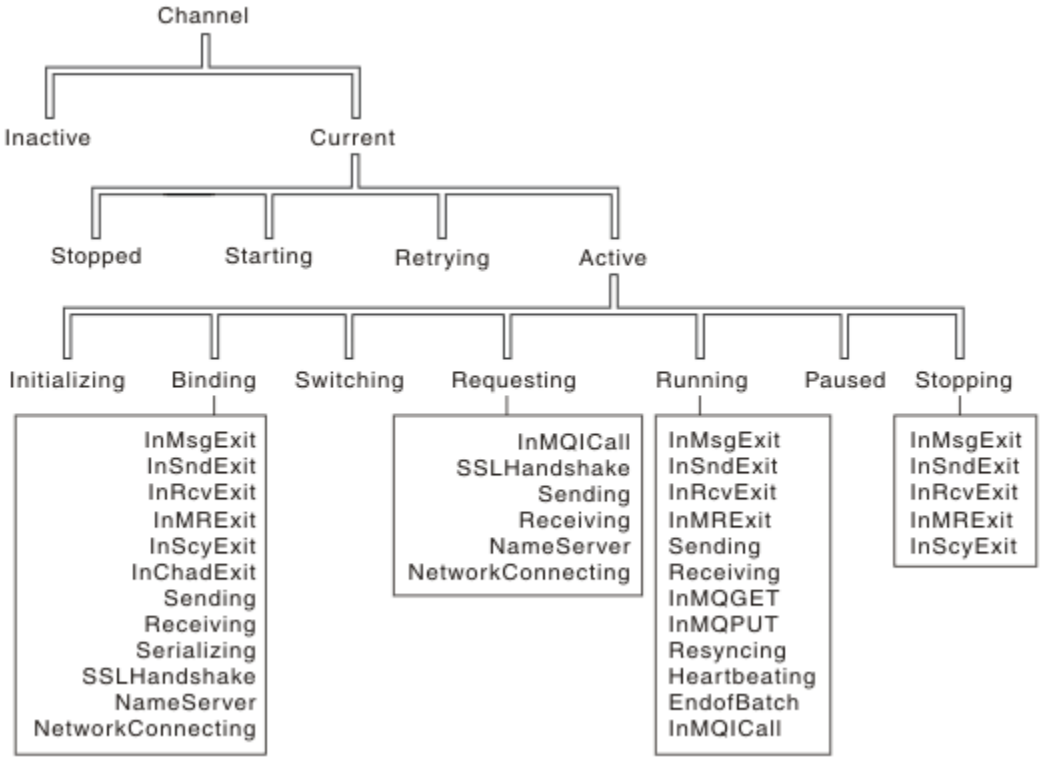
Poznámka: Vzhledem k tomu, že kanál je 'spuštěn', nemusí nutně přenášet zprávy. Místo toho může být 'povoleno' spustit přenos, když se vyskytne jedna ze čtyř událostí popsaných dříve. Povolení a zakázání kanálu je dosaženo pomocí příkazů operátorů START a STOP.

Stavy kanálů

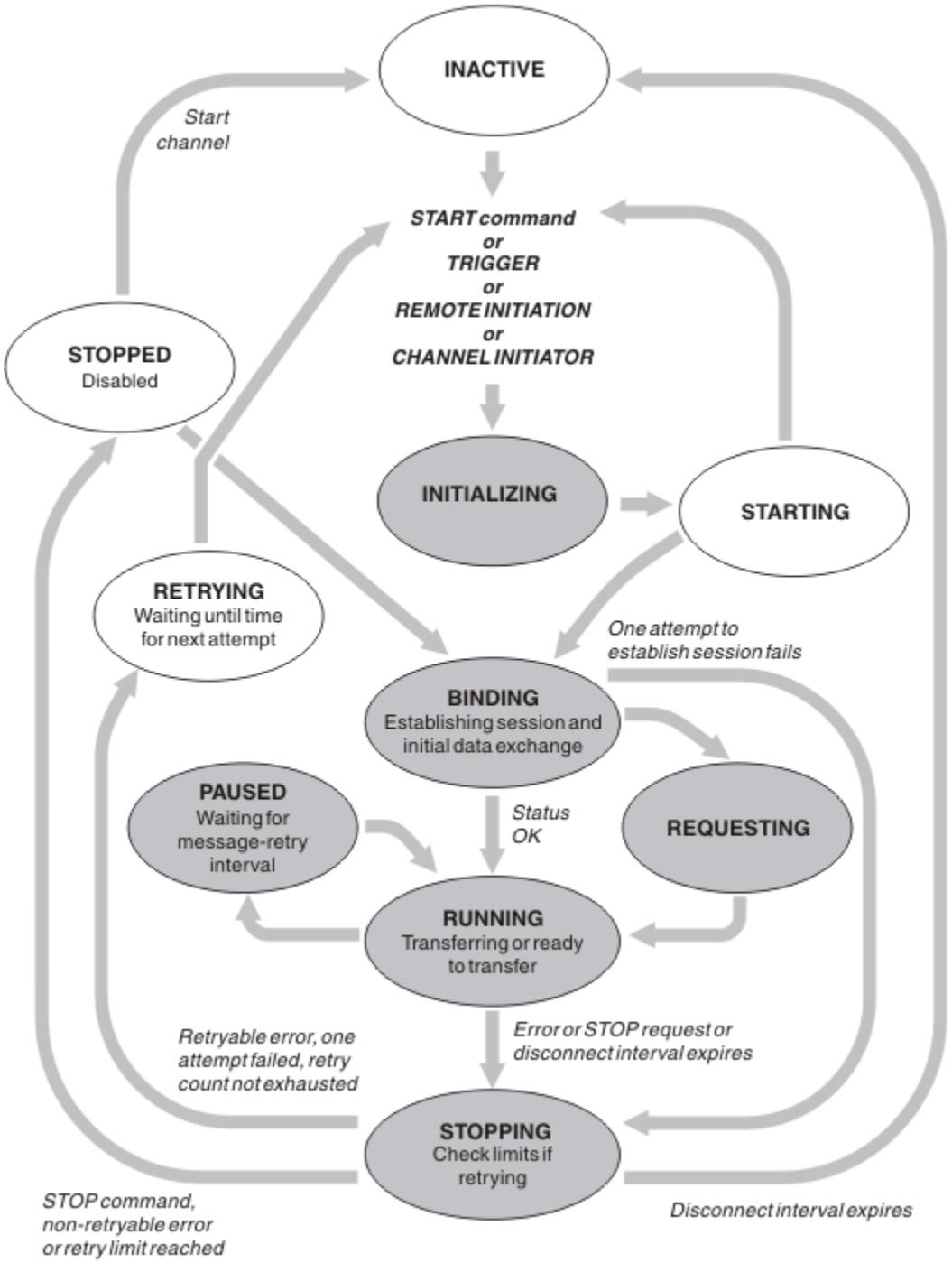
Kanál může být v libovolném okamžiku v některém z mnoha stavů. Některé stavy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

Obrázek 12 na stránce 55 zobrazuje hierarchii všech možných stavů kanálů a podstavů, které se vztahují ke každému z kanálů kanálu.

Obrázek 13 na stránce 56 zobrazuje odkazy mezi stavy kanálů. Tyto odkazy se vztahují na všechny typy kanálů zpráv a kanálů připojení k serveru.



Obrázek 12. Stavy kanálů a podstavy



Obrázek 13. Toky mezi stavy kanálů

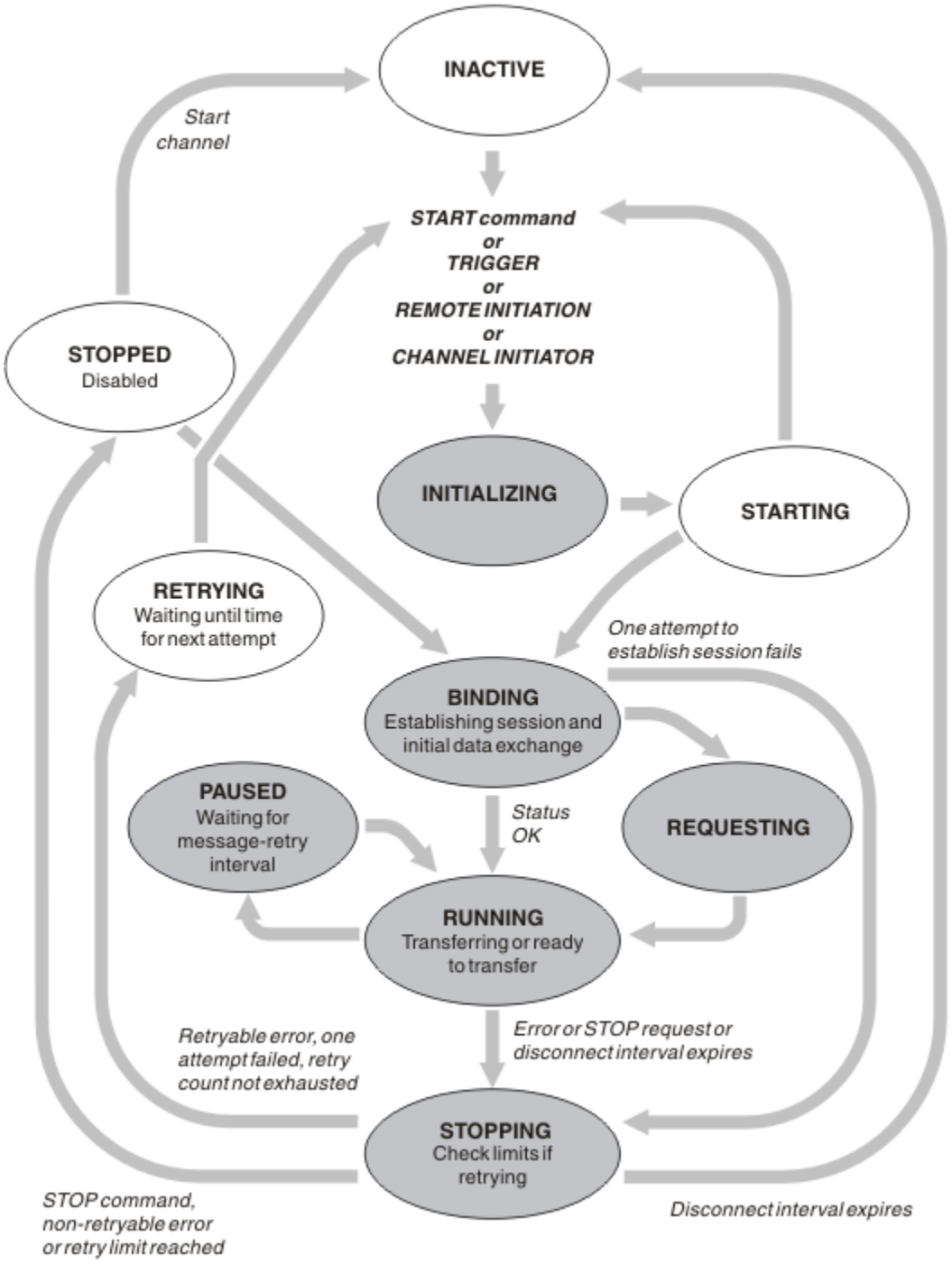
Aktuální a aktivní

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 části Obrázek 13 na stránce 56.

Aktivní kanál může také zobrazit podstav poskytující více podrobností přesně toho, co kanál dělá. Podstavy pro každý stav jsou zobrazeny v Obrázek 12 na stránce 55.

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 14. Toky mezi stavy kanálů

Poznámka:

1. Je-li kanál v jednom ze šesti stavů zvýrazněných v produktu Obrázek 14 na stránce 57 (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 konfigurační soubor správce front pro systémy UNIX and Linux nebo Průzkumníka WebSphere MQ . 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 produktu IBM WebSphere MQ pro WebSphere MQ pro systémy UNIX and Linux a systémy Okna.

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 spouštěn 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 zprávu, zapíše se zpráva do protokolu 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 produktu IBM WebSphere MQ for WebSphere MQ pro systémy UNIX and Linux a systémy Okna.

Chyby kanálu
Chyby na kanálech způsobí, že kanál zastaví další přenosy. Je-li kanálem odesilatel 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 restartovat (viz “Restartování zastavených kanálů” na stránce 62).

Poznámka: Pro systémy 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 správce front zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován, když je restartován správce front . Stav kanálu pro typ kanálu SVRCONN se však znovu nastaví, pokud se zastaví správce front , zatímco kanál je 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**.

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 vyčerpat 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.

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 WebSphere MQ pro systémy UNIX, Linuxa Windows používáte protokol TCP jako přenosový protokol, můžete nastavit volbu `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 (KAINT).

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 KAINT 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 produktu WebSphere MQ pro systémy UNIX, Linuxa systémy Windows je hodnota *vypršení časového limitu pro příjem* nastavena takto:

1. Pro počáteční počet toků před každým dohadování je hodnota *time-out* dvojnásobná než hodnota HBINT z definice kanálu.
2. Poté, co kanály vyjednají 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.

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 WebSphere 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*HBINT pro HBINTS menší než 60 sekund a 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 WebSphere MQ Explorer zrušit přijímací kanál a spustit nový na jeho místě.

Pokud kanál trpí selháním komunikace, může být kanál příjemce ponechán ve stavu 'příjem komunikací'. Když je komunikace znovu zavedena, kanál odesílatele se pokusí znovu navázat spojení. Pokud vzdálený správce front zjistí, že je kanál příjemce již spuštěn, není povoleno spuštění jiné verze téhož kanálu příjemce. Tento problém vyžaduje zásah uživatele k nápravě problému nebo použití systému keepalive.

Funkce Převzetí MCA řeší problém automaticky. Umožňuje IBM WebSphere MQ Explorer kanálu příjemce zrušit kanál příjemce a spustit nový jeho místo.

Funkci lze nastavit s různými volbami. distributed Pro distribuované platformy viz téma Administrace.

Zastavení a uvedení kanálů do klidového stavu

Toto téma vysvětluje, jak můžete zastavit a uvést kanál do klidového stavu před vypršením časového intervalu odpojení.

Kanály zpráv jsou navrženy tak, aby byly přerušitelné spojení mezi správci front se spořádaným ukončením řízeným pouze atributem kanálu přerušení připojení. Tento mechanizmus 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 WebSphere MQ

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.

TERMINATE
Volba TERMINATE se pokusí zastavit kanál okamžitě a ukončí vlákno nebo proces kanálu.

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 přerušení 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.

Chcete-li kanál znovu spustit, zadejte jeden z následujících příkazů:

- Příkaz START CHANNEL MQSC
- Příkaz Spuštění kanálu PCF
- Průzkumník IBM WebSphere MQ

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 správce front (na distribuovaných platformách) zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován, je-li restartován správce front . Stav kanálu pro typ kanálu SVRCONN se však resetuje, pokud se zastaví správce front, zatímco je 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 směrovat 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 příjemky, 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 WebSphere 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 produktu WebSphere MQ for IBM ilze příkaz DISPLAY CHSTATUS provést ze souboru pomocí příkazu STRMQMMQSC nebo příkazu WRKMQMCHST (Práce se stavem kanálu MQM).
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)
   ```

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 vracejí do terminálu, který inicioval příkazy, je-li to možné.

Produkt WebSphere MQ vytváří evidenční a statistické údaje, které lze použít k identifikaci trendů v oblasti využití a výkonu. distributed Na distribuovaných platformách jsou tyto informace vytvářeny jako záznamy PCF, podrobné informace viz Datové typy Structure .

Zprávy a kódy

Informace o zprávách a kódech, které vám pomohou s primární diagnózou problému, najdete v tématu Diagnostické zprávy a kódy příčin.

Bezpečnost zpráv

Kromě typických funkcí zotavení produktu WebSphere 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 vyřazováním
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 Nedodtrvalá 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.

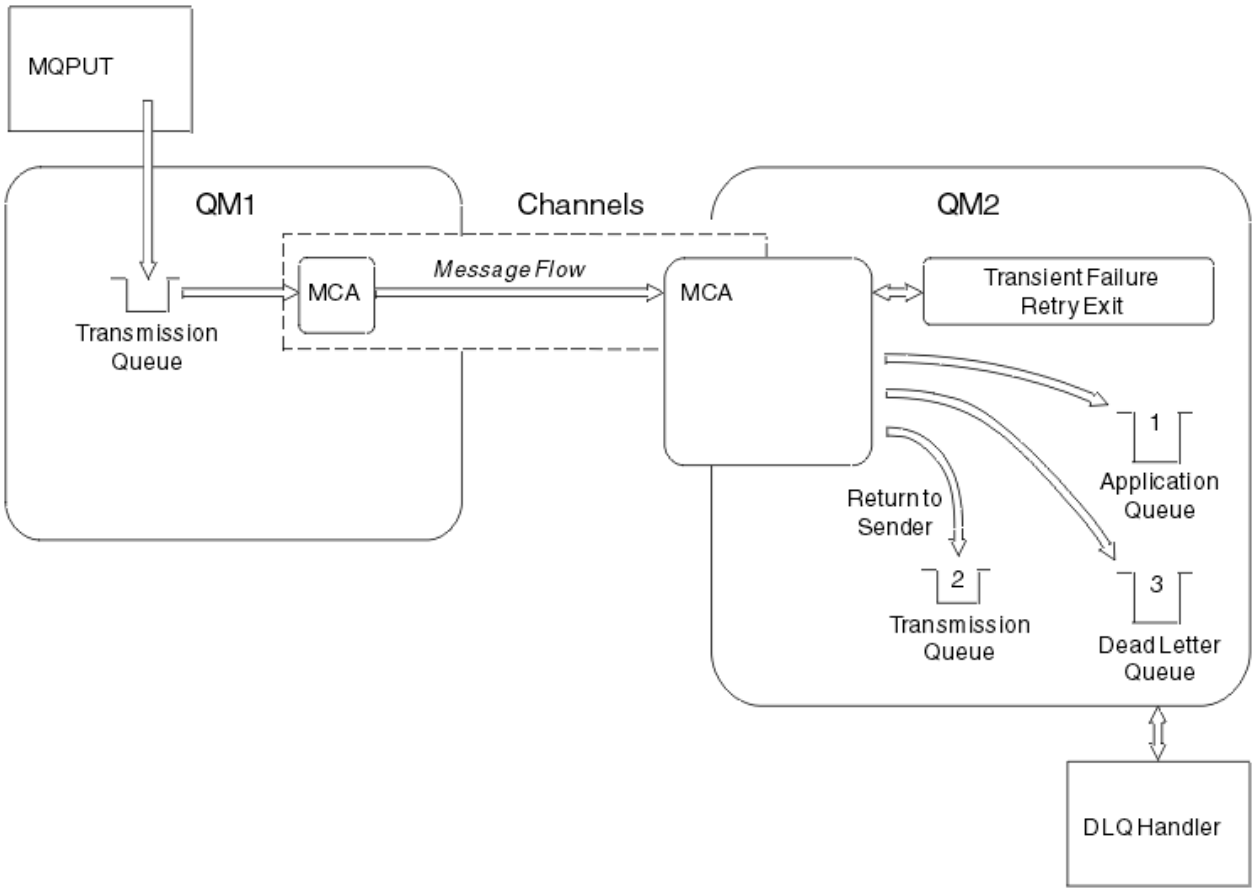
Nedoručené zprávy

Další informace o tom, co se stane, když nelze doručit zprávu, naleznete v části “Co se stane, když nebude možné zprávu doručit?” na stránce 64.

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 odesilateli, nebo to může dát do fronty nedoručených zpráv.

Obrázek 15 na stránce 65 uvádí zpracování, které se vyskytne, když agent MCA nemůže vložit zprávu do cílové fronty. (Zobrazené volby se nepoužijí na všechny platformy.)



Obrázek 15. 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 odesilateli

   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 odesilateli, 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 správci 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 Zpracování nedoručených zpráv s obslužnou rutinou fronty nedoručených zpráv produktu WebSphere MQ pro IBM WebSphere MQ for UNIX, Linux. 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 Version 7.0není 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 odkazy

Použít frontu nedoručených zpráv (USEDLQ)

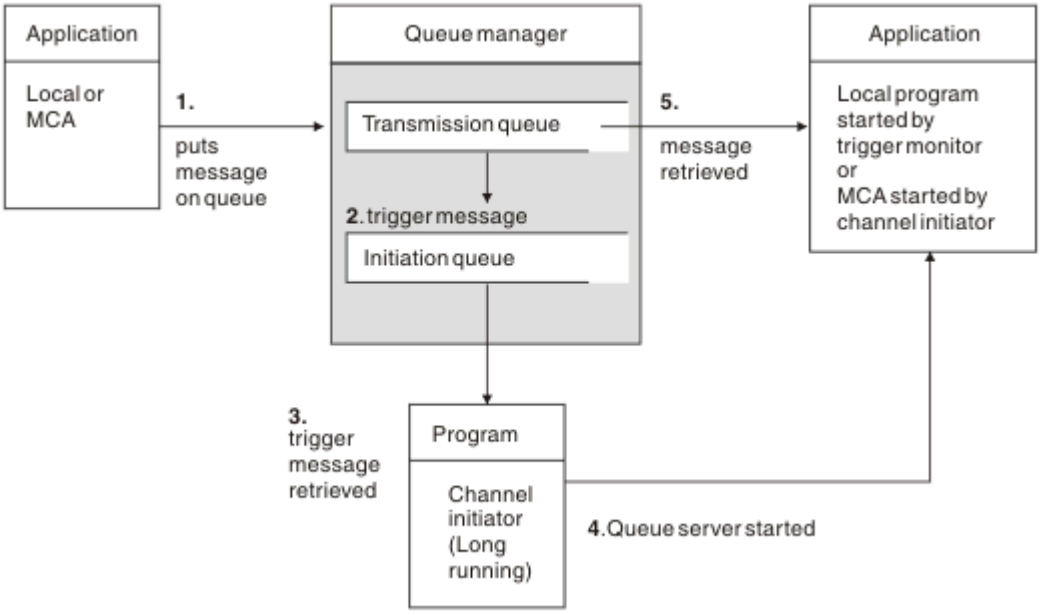
Spouštěcí kanály

Produkt WebSphere 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 WebSphere MQ pomocí spouštěčů.

Informace specifické pro danou platformu naleznete v následujících tématech:

- Pro Windowsviz systémy UNIX and Linux , “Spouštění kanálů na systémech UNIX, Linux a Windows .” na stránce 67



Obrázek 16. Koncepty spouštění

Objekty požadované pro spuštění jsou zobrazeny v Obrázek 16 na stránce 66. 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.
- 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. WebSphere MQ pro systémy UNIX, Linux a Windows umožňují, aby byl název kanálu zadán jako prázdný. V takovém případě bude použita 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. Řídicí 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 spouštění 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 inicializacím kanálu.

Spouštění kanálů na systémech UNIX, Linux a Windows .

Můžete vytvořit definici procesu v produktu WebSphere 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 pro systémy WebSphere MQ pro systémy 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 nezadáte název kanálu, bude inicializátor kanálu hledat v souborech definice kanálu, dokud nenajde kanál, který je přidružen k uvedené přenosové frontě.

Související pojmy

"Spuštění a zastavení inicializátoru kanálu" na stránce 68
Spouštěcí impuls je implementován pomocí procesu inicializátoru kanálu.

"Připojování aplikací pomocí distribuovaných front" na stránce 27
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu WebSphere MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související odkazy

Kanálové programy na systémech UNIX, Linuxa Windows

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 systému Linux a systémy Windows je inicializátor kanálu spuštěn automaticky. Počet inicializátorů kanálu, které lze spustit, je omezen. Výchozí a současně maximální hodnota je 3. Toto můžete změnit pomocí MAXINITIATORS v souboru qm.ini pro systémy UNIX and Linux a v registru pro systémy Windows.

Podrobnosti o příkazu spuštění inicializátoru kanálu **runmqchi**a o dalších řídicích příkazech najdete v části Příkazy řízení produktuWebSphere 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

Zpracování inicializačních dat kanálu závisí na použité platformě WebSphere MQ .

Windows, systémy UNIX and Linux

V produktu WebSphere MQ for Windows, UNIX and Linux jsou k dispozici *konfigurační soubory* , které obsahují základní informace o konfiguraci instalace produktu WebSphere MQ .

Existují dva konfigurační soubory: jedno platí pro daný počítač, druhé platí pro jednotlivého správce front.

Konfigurační soubor produktu WebSphere MQ
Tento soubor obsahuje informace vztahující se ke všem správcům front v systému WebSphere MQ . Soubor se nazývá mqs.ini. Je plně popsán v příručce Administrace pro produkt WebSphere MQ for Windows, UNIX and Linux systémů.

Konfigurační soubor správce front

Tento soubor obsahuje informace o konfiguraci týkající se jednoho konkrétního správce front. 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 výchozího nastavení v konfiguračním souboru produktu WebSphere 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 UNIX and 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 systémy Windows :

```
C:\Program Files\IBM\WebSphere MQ\qmgrs\QMNAME\qm.ini
```

Další informace o souborech qm.ini naleznete v tématu Stanzy konfiguračního souboru pro distribuované ukládání do fronty.

Převod dat pro zprávy

Zprávy produktu WebSphere MQ mohou vyžadovat převod dat při odesílání mezi frontami v různých správcích front.

Zpráva produktu WebSphere 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

Produkt WebSphere MQ umožňuje psát 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 WebSphere MQ pracoval v rámci vašeho vlastního patentovaného komunikačního protokolu nebo aby odesílal zprávy prostřednictvím protokolu, který produkt WebSphere MQ nepodporuje. (Chcete-li spolupracovat s produktem WebSphere MQ-dodaným agentem MCA na druhém konci, nemůžete napsat vlastní program MCA.)

Pokud se rozhodnete použít agenta MCA, který nebyl dodán produktem WebSphere 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.

Řídicí funkce kanálu
Chcete-li řídit kanály, musíte zadat své vlastní administrativní funkce. Administrační funkce kanálu produktu WebSphere MQ nelze použít pro konfiguraci (například příkaz DEFINE CHANNEL) nebo 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 umisťuje, například k přenosové frontě.

Uživatelské procedury
Zvažte, zda nepotřebujete uživatelské procedury. Pokud tomu tak je, můžete použít stejné definice rozhraní, které používá produkt WebSphere MQ .

Spouątění
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 vzít v úvahu při přípravě produktu WebSphere 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 WebSphere MQ na systémech UNIX and Linux ; další informace viz Ukázkový obslužný program DLQ, amqsdlq.

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

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 WebSphere MQ, ale lze je poskytovat v každé instalaci podle místních požadavků.

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 v systému UNIX, Linux, and Windows

Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, IBM WebSphere MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro informace o synchronizaci.

Můžete použít následující typy příkazů:

Příkazy IBM WebSphere MQ (MQSC)
Prostředí MQSC můžete použít jako jednotlivé příkazy v relaci MQSC v systémech Windows, UNIX and 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 WebSphere 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

Řídicí příkazy
Pro některé z těchto funkcí můžete také zadat příkaz *control commands* na příkazovém řádku. Další informace viz řídicí příkazy.

Formátovací příkazy Programovatelného příkazu
Podrobnosti naleznete v tématu Příkazy PCF.

IBM WebSphere MQ Explorer
V systémech UNIX, Linux a Windows můžete použít produkt IBM WebSphere MQ Explorer. 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 8 na stránce 73.

Související pojmy

“Začínáme s objekty” na stránce 75
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 systém Windows” na stránce 81
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. This section explains how to do this using one of the four forms of communication for WebSphere MQ for Okna systems.

“Nastavení komunikace v systémech UNIX and Linux” na stránce 90
DQM je prostředek vzdáleného řazení do fronty pro produkt IBM WebSphere 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.

Související odkazy

Kanálové programy na systémech UNIX, Linuxa Windows

Příklad plánování kanálů zpráv pro distribuované platformy

Příklad konfiguračních informací

Funkce vyžadované pro nastavení a řízení kanálů

Pro nastavení a řízení kanálů může být zapotřebí řada funkcí IBM WebSphere MQ . Funkce kanálu jsou vysvětleny v tomto tématu.

Definici kanálu můžete vytvořit s použitím výchozích hodnot dodaných produktem IBM WebSphere 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 WebSphere MQ .

Informace o dalších funkcích souvisejících s kanálem naleznete v následujících tématech:

- “Začínáme s objekty” na stránce 75
- “Vytváření přidružených objektů” na stránce 75
- “Vytváření výchozích objektů” na stránce 75
- “Vytvoření kanálu” na stránce 76
- “Zobrazení kanálu” na stránce 76
- “Zobrazení stavu kanálu” na stránce 77
- “Kontrola odkazů pomocí příkazu ping” na stránce 77
- “Spuštění kanálu” na stránce 78
- “Zastavení kanálu” na stránce 79
- “Přejmenování kanálu” na stránce 80
- “Resetování kanálu” na stránce 80
- “Vyřešení nejistých zpráv na kanálu” na stránce 80

Produkt Tabulka 8 na stránce 73 zobrazí úplný seznam funkcí produktu IBM WebSphere MQ , které můžete potřebovat.

Tabulka 8. Funkce vyžadované v systémech UNIX, Linux, and Windows

Funkce	**Řídicí příkazy**	**MQSC**	**Ekvivalent v produktu WebSphere MQ Explorer?**
Funkce správce front			
Změnit správce front		ALTER QMGR	Ano
Vytvoření správce front	crtmqm		Ano
Odstranit správce front	dltmqm		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

Tabulka 8. Funkce vyžadované v systémech UNIX, Linux, and Windows (pokračování)			
Funkce	**Řídicí příkazy**	**MQSC**	**Ekvivalent v produktu WebSphere MQ Explorer?**
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
Odstranit frontu		VÝMAZ QALIAS DELETE QLOCAL DELETE QMODEL DELETE QREMOTE Viz DELETE queues .	Ano
Zobrazit frontu		ZOBRAZIT FRONTU	Ano
funkce procesu			
Změnit proces		ZMĚNA PROCES	Ano
Vytvořit proces		DEFINOVAT PROCES	Ano
Odstranit proces		Odstranit proces	Ano
Zobrazit proces		ZOBRAZIT PROCES	Ano
Funkce kanálu			
Změnit kanál		ALTER CHANNEL	Ano
Vytvořit kanál		Definovat kanál	Ano
Odstranit kanál		Odstranit kanál	Ano
Zobrazit kanál		DISPLAY CHANNEL	Ano
Zobrazit stav kanálu		ZOBRAZIT STAV CHSTATUS	Ano
Ukončit kanál		Ukončit kanál	Ano
Odeslat signál Ping pro kanál		Odeslat signál Ping pro kanál	Ano
Resetovat kanál		Resetovat kanál	Ano
Vyřešit kanál		Vyřešit kanál	Ano

Tabulka 8. Funkce vyžadované v systémech UNIX, Linux, and Windows (pokračování)			
Funkce	**Řídicí příkazy**	**MQSC**	**Ekvivalent v produktu WebSphere MQ Explorer?**
Spustit kanál	runmqchl	Spustit kanál	Ano
Spustit inicializátor kanálu	runmqchi	START CHINIT	Ne
Spustit modul listener[1]	runmqlsr	Spustit listener	Ne
Koncový modul listener	endmqlsr (pouze systémy Windows , AIX, HP-UXa 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 WebSphere MQ (MQSC) nebo IBM WebSphere MQ Explorer 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 odpovědí
- 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 odpovědí 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 Řídicí 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 vytvoříte 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: Odesilatel 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') +
CONNAME(QM2) TRPTYPE(TCP) XMITQ(QM2) CONVERT(YES)
```

Ve všech příkladech příkazů 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 lze položku ukončit na příkazovém řádku pomocí kláves Ctrl-z. Na systémech UNIX and Linux použijte klávesu Ctrl-d. Případně můžete na systémech UNIX, Linux nebo Windows použít 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 podprocesu (pouze systém 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 z odesílacích kanálů a kanálů serveru. 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 WebSphere 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 UNIX and Linux může být démon inetd konfigurován pro spuštění kanálu. inetd se spouští jako oddělený proces.
- Pro LU 6.2 v systémech UNIX and Linux nakonfigurujte svůj produkt SNA tak, aby spustil proces odpovídacího modulu LU 6.2 .
- Pro LU 6.2 v systémech Windows pomocí serveru SNA můžete ke spuštění kanálu použít program TpStart (obslužný program dodávaný se serverem SNA). 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 spuštění, 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, do kterého je produkt WebSphere MQ nainstalován.

Poznámka: Na systémech Windows se stále také zobrazí zpráva v protokolu událostí aplikace systému Windows .

Systémy UNIX and 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)

V systémech Windows, UNIX and Linux , použijte příkaz runmqlsr ke spuštění procesu modulu listener produktu WebSphere MQ . Při výchozím nastavení všechny příchozí požadavky na připojení kanálu způsobí spuštění modulu listener MCA jako podprocesy procesu amqrmppa.

```
runmqlsr -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 naleznete v tématu “Restartování zastavených kanálů” na stránce 62.

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 75
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.

“Řídicí funkce kanálu” na stránce 52
Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

“Připojování aplikací pomocí distribuovaných front” na stránce 27
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu WebSphere MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související odkazy

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 odesilatel nebo server
- Definice lokálního kanálu musí existovat
- Lokální správce front musí být spuštěn.

Související pojmy

"Začínáme s objekty" na stránce 75
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.

"Řídicí funkce kanálu" na stránce 52
Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

"Připojování aplikací pomocí distribuovaných front" na stránce 27
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu WebSphere MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související odkazy

Vyřešit kanál

Nastavení komunikace pro systém 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. This section explains how to do this using one of the four forms of communication for WebSphere MQ for Okna systems.

Může být užitečné se podívat na téma Příklad konfigurace- IBM WebSphere MQ for Windows.

Informace o systémech UNIX and Linux naleznete v části "Nastavení komunikace v systémech UNIX and Linux" na stránce 90.

Rozhodování o připojení

Vyberte si z následujících čtyř forem komunikace pro WebSphere MQ pro systémy Okna :

- "Definování připojení TCP na systému Windows" na stránce 82
- "Definování připojení LU 6.2 na systému Windows" na stránce 83
- "Definování připojení NetBIOS v systému Windows" na stránce 85
- "Definování připojení SPX v systému Windows" na stránce 88 (pouze systémy Windows XP a Windows 2003 Server)

Každá definice kanálu musí určovat pouze jeden protokol jako atribut Přenosový protokol (Typ transportu). Jeden nebo více protokolů může správce front použít.

Pro klienty WebSphere MQ může být užitečné mít alternativní kanály používající různé přenosové protokoly. Další informace o klientech WebSphere MQ naleznete v tématu Přehled klientů.

Související pojmy

"Připojování aplikací pomocí distribuovaných front" na stránce 27
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu WebSphere MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

"Monitorování a řízení kanálů v systému UNIX, Linux, and Windows" na stránce 72
Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, IBM WebSphere MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro informace o synchronizaci.

“Konfigurace připojení mezi klientem a serverem” na stránce 96
Chcete-li konfigurovat komunikační spojení mezi klienty a servery produktu WebSphere MQ MQI, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích propojení, 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 oprávněním Internet Assigned Numbers Authority k IBM WebSphere 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) +
          CONNAME('OS2ROG3(1822)') +
          XMITQ('XMitQ name') +
          REPLACE
```

kde OS2ROG3 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 změna definice objektu kanálu.

Výchozí číslo portu můžete změnit tak, že jej uvedete v souboru `.ini` pro IBM WebSphere MQ pro Windows:

```
TCP:
Port=1822
```

Poznámka: Chcete-li vybrat číslo portu TCP/IP, které se má použít, použije produkt IBM WebSphere 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 WebSphere 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 WebSphere 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 WebSphere MQ .

Chcete-li spustit modul listener dodávaný s produktem IBM WebSphere MQ, který spouští nové kanály jako podprocesy, použijte příkaz runmqlsr .

Základní příklad použití příkazu **runmqlsr** :

```
runmqlsr -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, použije produkt IBM WebSphere 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 WebSphere MQ úřadem Internet Assigned Numbers Authority pro příchozí i odchozí připojení.

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM WebSphere MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu “Spuštění kanálů a listenerů jako důvěryhodných aplikací” na stránce 71. 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 60.

V systému Windowshodnota registru `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` pro volbu času Windows KeepAliveřídí interval, který uplyne, než se bude kontrolovat připojení. Výchozí hodnota je dvě hodiny.

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.

Tabulka 9. Nastavení na lokálním systému Windows pro vzdálenou platformu správce front

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 používající CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-
IBM i	Stejné jako porovnávací hodnota v záznamu směrování v systému IBM i .	-
Systémy UNIX and Linux	Totéž jako v příslušných vedlejších informacích o vzdáleném správci front.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a

Tabulka 9. Nastavení na lokálním systému Windows pro vzdálenou platformu správce front (pokračování)		
Vzdálená platforma	**TPNAME**	**TPPATH.**
Windows	Jak je uvedeno v příkazu Windows Run Listener, nebo na nepřevolaném transakčním programu, který byl definován pomocí volby TpSetup v systému Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

MQ_INSTALLATION_PATH představuje adresář vysoké úrovně, v němž je nainstalován produkt WebSphere MQ .

Pokud máte na jednom počítači více než jednoho správce front, ujistěte se, že názvy TPnames v definicích kanálů jsou jedinečné.

Nejnovější informace o konfiguraci protokolu AnyNet SNA přes TCP/IP najdete v následující online dokumentaci IBM : AnyNet SNA přes TCP/IP a Obsluha uzlu SNA.

Související pojmy

“Odeslání konce LU 6.2” na stránce 84
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 84
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              OS2ROG2
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 použít TpStart pod serverem SNA for Windows.

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 WebSphere MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu Spuštění kanálů a listenerů jako důvěryhodných aplikací. Informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

Všechny moduly listener produktu WebSphere MQ spuštěné ve správci front, který je neaktivní, můžete zastavit pomocí příkazu:

```
ENDMQLSR [-m QMNAME]
```

Použití serveru Microsoft SNA Server v 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 WebSphere MQ používá tři typy prostředků NetBIOS při vytváření připojení NetBIOS k jinému produktu WebSphere 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 produktu IBM NetBIOS umožňuje více procesům používat stejný lokální název NetBIOS . Proto musí být k dispozici pouze jeden název NetBIOS pro použití produktem WebSphere 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 zvyšte 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 WebSphere MQ potřebuje získat. Administrátor sítě LAN by vám to měl být schopen objasnit.

Související pojmy

“Definování lokálního názvu NetBIOS produktu IBM WebSphere MQ” na stránce 86
Lokální název NetBIOS použitý procesy kanálu IBM WebSphere MQ lze zadat třemi způsoby.

“Vytváření omezení relací, příkazů a názvů správce front NetBIOS” na stránce 86
Omezení správce front pro relace NetBIOS , příkazy a názvy lze zadat dvěma způsoby.

“Zavedení čísla adaptéru LAN” na stránce 87
Aby kanály fungovaly úspěšně napříč protokolem NetBIOS, musí být podpora adaptéru na každém konci kompatibilní. IBM WebSphere 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.

“Inicializace připojení NetBIOS” na stránce 87
Definování kroků potřebných k zahájení připojení.

“Cílový modul listener pro připojení NetBIOS” na stránce 87
Definování kroků, které mají být provedeny na přijímajícím konci připojení NetBIOS .

Definování lokálního názvu NetBIOS produktu IBM WebSphere MQ
Lokální název NetBIOS použitý procesy kanálu IBM WebSphere MQ lze zadat 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 WebSphere 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 Windowsnelze 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. IBM WebSphere 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 WebSphere MQ pro připojení NetBIOS je 0. Ověřte, jaké číslo se používá ve vašem systému, a to následujícím způsobem:

V systému Windowsnení možné zadávat dotazy na číslo adaptéru LAN přímo prostřednictvím operačního systému. Místo toho použijte LANACFG.EXE obslužný program příkazového řádku, dostupný od společnosti Microsoft. Výstup nástroje zobrazuje čísla virtuálních adaptérů LAN a jejich účinné vazby. Další informace o číslech adaptérů LAN najdete v článku 138037 znalostní báze Microsoft Knowledge Base *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) +
          CONNAME(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 modulu listener produktu WebSphere MQ zaveďte stanici a zpřístupníte 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 .

Nejlepších výsledků dosáhnete spuštěním modulu listener produktu WebSphere MQ jako důvěryhodné aplikace, jak je popsáno v tématu “Spuštění kanálů a listenerů jako důvěryhodných aplikací” na stránce 71. Informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

Všechny moduly listener produktu WebSphere MQ spuštěné ve správci front, který je neaktivní, můžete zastavit pomocí příkazu:

```
ENDMQLSR [-m QMNAME]
```

Nezadáte-li název správce front, bude předpokládán výchozí správce front.

Definování připojení SPX v systému Windows

Připojení SPX se vztahuje pouze na klienta a server se systémem Windows XP a Windows 2003 Server.

Definice kanálu na odesílajícím konci uvádí adresu cíle. Program modulu listener musí být spuštěn na přijímajícím konci.

Související pojmy

“Odesílání konce na SPX” na stránce 88
Je-li cílový počítač vzdálený, zadejte adresu SPX cílového počítače v poli Název připojení v definici kanálu.

“Příjem na SPX” na stránce 89
Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu.

“Parametry protokolu IPX/SPX” na stránce 90
Ve většině případů budou výchozí nastavení pro parametry IPX/SPX vyhovovat vašim potřebám. Může však být nutné upravit některé z nich ve vašem prostředí a vyladit její použití pro produkt WebSphere MQ.

Odesílání konce na SPX
Je-li cílový počítač vzdálený, zadejte adresu SPX cílového počítače v poli Název připojení v definici kanálu.

Adresa SPX je určena v následujícím tvaru:

```
        network.node(socket)
```

kde:

network
je 4bajtová síťová adresa sítě, na které je umístěn vzdálený počítač,

node
Je 6bajtová adresa uzlu, která je adresou LAN adaptéru LAN ve vzdáleném počítači

socket
Je 2bajtové číslo soketu, na kterém vzdálený počítač naslouchá.

Pokud jsou lokální a vzdálené počítače na stejné síti, pak není třeba uvést síťovou adresu. Pokud vzdálený konec naslouchá na výchozím soketu (5E86), pak nemusí být soket zadán.

Příklad plně zadané adresy SPX zadané v parametru CONNAME příkazu MQSC:

```
      CONNAME('00000001.08005A7161E5(5E87)')
```

Ve výchozím případě, jsou-li počítače ve stejné síti, se stane toto:

```
      CONNAME(08005A7161E5)
```

Výchozí číslo soketu lze změnit jeho určením v konfiguračním souboru správce front (qm.ini):

```
SPX:
  Socket=5E87
```

Další informace o hodnotách, které jste nastavili pomocí souboru qm.ini, najdete v tématu Stanzy konfiguračního souboru pro distribuované ukládání do fronty .

Příjem na SPX
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.

Použijte modul listener produktu WebSphere MQ .

Použití volby seznamu požadavků modulu listener SPX

Při příjmu na SPX je nastaven maximální počet neprovedených požadavků na připojení. To lze považovat za *nevyřízené požadavky* požadavků čekajících na port SPX, aby mohl modul listener přijmout požadavek. Výchozí hodnoty nevyřízených požadavků listeneru jsou zobrazeny v Tabulka 10 na stránce 89.

Tabulka 10. Výchozí nevyřízené požadavky na připojení v systému Windows

Platforma	**Výchozí hodnota nevyřízených požadavků listeneru**
Server Windows	5
Pracovní stanice Windows	5

Pokud se nevyřízené požadavky dostanou k hodnotám v produktu Tabulka 10 na stránce 89, zobrazí se při pokusu o připojení ke správci front pomocí MQCONN nebo MQCONNX kód příčiny MQRC_Q_MGR_NOT_AVAILABLE. Pokud k tomu dojde, je možné se pokusit o připojení znovu.

Chcete-li se však této chybě vyhnout, můžete přidat položku do souboru qm.ini nebo do registru systému Windows:

```
SPX:
ListenerBacklog = n
```

Tento parametr přepíše výchozí maximální počet nevyřízených požadavků (viz Tabulka 10 na stránce 89) pro modul listener SPX.

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí. Je-li to nutné, lze ji použít k tomu, abyste se vyhnuli dosažení limitu připojení.

Chcete-li spustit modul listener s volbou `backlog` , přepnete na:

- Použijte příkaz `RUNMQLSR -b` nebo
- Použijte příkaz MQSC **`DEFINE LISTENER`** s atributem BACKLOG nastaveným na požadovanou hodnotu.

Informace o příkazu **RUNMQLSR** naleznete v části runmqlsr. Další informace o příkazu DEFINE LISTENER naleznete v tématu DEFINE LISTENER.

Použití modulu listener produktu WebSphere MQ

Chcete-li spustit modul listener dodávaný s produktem WebSphere MQ, který spouští nové kanály jako podprocesy, použijte příkaz RUNMQLSR. Příklad:

```
RUNMQLSR -t spx [-m QMNAME] [-x 5E87]
```

Hranaté závorky označují volitelné parametry; `QMNAME` není vyžadováno pro výchozího správce front a číslo soketu není povinné, pokud používáte výchozí (5E86).

Nejlepších výsledků dosáhnete spuštěním modulu listener produktu WebSphere MQ jako důvěryhodné aplikace, jak je popsáno v tématu “Spuštění kanálů a listenerů jako důvěryhodných aplikací” na stránce 71. Další informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

Všechny moduly listener produktu WebSphere MQ spuštěné ve správci front, který je neaktivní, můžete zastavit pomocí příkazu:

```
ENDMQLSR [-m QMNAME]
```

Nezadáte-li název správce front, bude předpokládán výchozí správce front.

Parametry protokolu IPX/SPX
Ve většině případů budou výchozí nastavení pro parametry IPX/SPX vyhovovat vašim potřebám. Může však být nutné upravit některé z nich ve vašem prostředí a vyladit její použití pro produkt WebSphere MQ.

Skutečné parametry a metoda jejich změny se liší v závislosti na platformě a poskytovateli podpory komunikace SPX. Část příkladu popisuje některé z těchto parametrů, zejména ty, které mohou ovlivnit provoz kanálů a připojení klienta produktu WebSphere MQ .

systémy Windows

Podrobné informace o použití a nastavení parametrů NWLink IPX a SPX najdete v dokumentaci společnosti Microsoft . Parametry protokolu IPX/SPX se nacházejí v registru v následujících cestách:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\NWLinkSPX\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\NWLinkIPX\Parameters
```

Nastavení komunikace v systémech UNIX and Linux

DQM je prostředek vzdáleného řazení do fronty pro produkt IBM WebSphere 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.

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 WebSphere MQ for AIX
- Příklad konfigurace- IBM WebSphere MQ for HP-UX
- Příklad konfigurace- IBM WebSphere MQ for Solaris
- Příklad konfigurace- IBM WebSphere MQ for Linux

Pro systémy Windowsviz “Nastavení komunikace pro systém Windows” na stránce 81.

Můžete si vybrat mezi dvěma způsoby komunikace pro produkt WebSphere MQ na systémech UNIX and Linux :

- “Definování připojení TCP na systému UNIX and Linux” na stránce 91
- “Definování připojení LU 6.2 na serveru UNIX and Linux” na stránce 94

Každá definice kanálu musí určovat jeden pouze jako atribut přenosového protokolu (Typ transportu). Jeden nebo více protokolů může správce front použít.

Pro klienty IBM WebSphere MQ Explorer MQI může být užitečné mít alternativní kanály používající různé přenosové protokoly. Další informace o klientech IBM WebSphere MQ Explorer MQI naleznete v tématu Přehled klientů IBM WebSphere MQ MQI .

Související pojmy
“Připojování aplikací pomocí distribuovaných front” na stránce 27
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu WebSphere MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

“Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 72

Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, IBM WebSphere MQ Explorer, souborů pro definice kanálů a oblastí úložiště pro informace o synchronizaci.

“Konfigurace připojení mezi klientem a serverem” na stránce 96
Chcete-li konfigurovat komunikační spojení mezi klienty a servery produktu WebSphere MQ MQI, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích propojení, spusťte modul listener a definujte kanály.

Definování připojení TCP na systému UNIX and 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 oprávněním Internet Assigned Numbers Authority k produktu WebSphere 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 démonem inet (inetd), nebo modul listener produktu WebSphere 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 92
Chcete-li spustit kanály v systému UNIX and Linux, je třeba upravit soubor /etc/services a soubor inetd.conf .

“Použití volby nevyřízených požadavků na modul listener TCP” na stránce 93
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 WebSphere MQ” na stránce 94
Chcete-li spustit modul listener dodávaný s produktem WebSphere MQ, který spouští nové kanály jako podprocesy, použijte příkaz `runmqlsr` .

“Použití volby TCP/IP SO_KEEPALIVE” na stránce 94
Na některých systémech UNIX and 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 UNIX and 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 přihlášeni 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 WebSphere 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, do kterého je produkt WebSphere MQ instalován:

   ```
   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:

- V systému AIX:

  ```
  refresh -s inetd
  ```
- V systému HP-UXz ID uživatele mqm:

  ```
  inetd -c
  ```
- V systému Solaris 10 nebo novějším:

  ```
  inetconv
  ```
- Na jiných systémech UNIX and 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 produktu WebSphere 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 do národního prostředí použitého pro ostatní procesy produktu WebSphere 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, do kterého je produkt WebSphere MQ nainstalován.

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 93.

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 modulu listener jsou zobrazeny v části Tabulka 11 na stránce 93.

Tabulka 11. 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 i	255
Solaris	100
Server Windows	100
Pracovní stanice Windows	100
z/OS	255

Pokud se nahromadění nevyřízených požadavků dosáhne hodnot zobrazených v produktu Tabulka 11 na stránce 93, 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 11 na stránce 93) 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 `runmqlsr -b` nebo
- Použijte příkaz MQSC **`DEFINE LISTENER`** s atributem BACKLOG nastaveným na požadovanou hodnotu.

Informace o příkazu **runmqlsr** naleznete v části runmqlsr. Další informace o příkazu DEFINE LISTENER naleznete v tématu DEFINE LISTENER.

Použití modulu listener produktu WebSphere MQ
Chcete-li spustit modul listener dodávaný s produktem WebSphere MQ, který spouští nové kanály jako podprocesy, použijte příkaz `runmqlsr` .

Příklad:

```
runmqlsr -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.

Nejlepších výsledků dosáhnete spuštěním modulu listener produktu WebSphere MQ jako důvěryhodné aplikace, jak je popsáno v tématu “Spuštění kanálů a listenerů jako důvěryhodných aplikací” na stránce 71. Informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

Všechny moduly listener produktu WebSphere MQ spuštěné ve správci front, který je neaktivní, můžete zastavit pomocí příkazu:

```
endmqlsr [-m QMNAME]
```

Nezadáte-li název správce front, bude předpokládán výchozí správce front.

Použití volby TCP/IP SO_KEEPALIVE
Na některých systémech UNIX and 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 60), musíte přidat následující položku do konfiguračního souboru správce front (qm.ini):

```
TCP:
   KeepAlive=yes
```

Další informace naleznete v dokumentaci k systému UNIX and Linux .

Definování připojení LU 6.2 na serveru UNIX and 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.

Tabulka 12. Nastavení na lokálním systému UNIX and Linux pro vzdálenou platformu správce front

Vzdálená platforma	**TPNAME**	**TPPATH.**
z/OS bez CICS	Stejné jako odpovídající TPName v informacích o připojení vzdáleného správce front.	-
z/OS pomocí CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-

Tabulka 12. Nastavení na lokálním systému UNIX and Linux pro vzdálenou platformu správce front (pokračování)

Vzdálená platforma	**TPNAME**	**TPPATH.**
IBM i	Stejné jako porovnávací hodnota v záznamu směrování v systému IBM i .	-
Systémy UNIX and Linux	Stejné jako odpovídající TPName v informacích o připojení vzdáleného správce front.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a
Windows	Jak je uvedeno v příkazu Windows Run Listener, nebo na nepřevolaném transakčním programu, který byl definován pomocí volby TpSetup v systému Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

MQ_INSTALLATION_PATH představuje adresář vysoké úrovně, do kterého je produkt WebSphere MQ nainstalován.

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 95
V systému UNIX and 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 95
Na systémech UNIX and Linux vytvořte naslouchací přílohu na přijímajícím konci, profil logické připojení LU 6.2 a profil TPN.

Odesílání: Konec
V systému UNIX and 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-UXpoužijte k pojmenování lokální LU, kterou by měl odesílatel používat, proměnnou prostředí APPCLLU. V systému Solaris nastavte proměnnou prostředí APPC_LOCAL_LU na název lokální LU.

V případě, že produkt WebSphere MQ naváže relaci SNA, je použit parametr SECURITY PROGRAM, je-li podporován systémem CPI-C.

Příjem na LU 6.2
Na systémech UNIX and 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, do kterého je produkt WebSphere MQ nainstalován.

V systémech, kde můžete nastavit ID uživatele, zadejte uživatele, který je členem skupiny mqm.
V systému AIX, Solaris a HP-UXnastavte proměnné prostředí APPCTPN (název transakce) a APPCLLU (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.

Konfigurace připojení mezi klientem a serverem

Chcete-li konfigurovat komunikační spojení mezi klienty a servery produktu WebSphere MQ MQI, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích propojení, spusťte modul listener a definujte kanály.

V produktu WebSphere MQse logická komunikační spojení mezi objekty nazývají *kanály*. Kanály používané pro připojení klientů MQI produktu WebSphere MQ k serverům se nazývají kanály MQI. Definice kanálů se nastavují na každém konci propojení tak, aby aplikace WebSphere MQ v klientu MQI WebSphere MQ mohla komunikovat se správcem front na serveru. Podrobný popis tohoto postupu naleznete v tématu Kanály definované uživatelem.

Před definováním kanálů MQI musíte:

1. Rozhodněte se, jakou formu komunikace budete používat. Viz “Jaký typ komunikace použít” na stránce 96.
2. Definujte připojení na každém konci kanálu:

   Chcete-li definovat připojení, musíte:

   - Nakonfigurujte připojení.
   - Zaznamenejte hodnoty parametrů, které potřebujete pro definice kanálů.
   - Spuštěním modulu *listener*povolte serveru zjišťovat příchozí síťové požadavky z klienta rozhraní MQI produktu WebSphere MQ .

Jaký typ komunikace použít

Různé platformy podporují různé přenosové protokoly. Volba přenosového protokolu závisí na kombinaci platformy klienta a serveru produktu WebSphere MQ MQI.

Pro kanály MQI existují až čtyři typy přenosových protokolů v závislosti na platformách klienta a serveru:

- LU 6.2
- NetBIOS
- SPX
- TCP/IP

Při definování kanálů MQI musí každá definice kanálu určovat atribut přenosového protokolu (typ přenosu). Server není omezen na jeden protokol, takže různé definice kanálů mohou určovat různé protokoly. Pro klienty MQI WebSphere MQ může být užitečné mít alternativní kanály MQI používající různé přenosové protokoly.

Výběr přenosového protokolu může být omezen konkrétní kombinací platforem klienta a serveru produktu WebSphere MQ MQI. Možné kombinace jsou uvedeny v následující tabulce.

Tabulka 13. Přenosové protokoly-kombinace platforem klienta a serveru produktu WebSphere MQ MQI		
Přenosový protokol	**WebSphere MQ Klient MQI**	**Server WebSphere MQ**
TCP/IP	Systémy UNIX Windows	Systémy UNIX Windows z/OS
LU 6.2	Systémy UNIX[1] Windows	Systémy UNIX[1] Windows
NetBIOS	Windows	Windows
SPX	Windows	Windows
Poznámka: 1. Kromě Linux pro Power Systems		

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

- “Definování připojení TCP na systému Windows” na stránce 82
- “Definování připojení TCP na systému UNIX and Linux” na stránce 91
- “limity připojení TCP/IP” na stránce 99
- “Definování připojení LU 6.2 na systému Windows” na stránce 83
- “Definování připojení LU 6.2 na serveru UNIX and Linux” na stránce 94
- “Definování připojení NetBIOS v systému Windows” na stránce 85
- “Definování připojení SPX v systému Windows” na stránce 88

Související pojmy

“Konfigurace rozšířeného transakčního klienta” na stránce 100
Tato kolekce témat popisuje, jak nakonfigurovat rozšířenou transakční funkci pro každou kategorii správce transakcí.

“Definování kanálů MQI” na stránce 109
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 110
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 113
Na serveru můžete vytvořit obě definice a potom zpřístupnit definici klienta-připojení klientovi.

“Programy pro ukončení kanálů pro kanály MQI” na stránce 118
Na systémech UNIX, Linux a Windows jsou k dispozici tři typy uživatelské procedury kanálu pro klientské prostředí WebSphere MQ MQI.

“Připojení klienta ke skupině sdílení front” na stránce 121
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 123
Nakonfigurujte klienty pomocí atributů v textovém souboru. Tyto atributy mohou být přepsány proměnnými prostředí nebo jinými způsoby specifickými pro platformu.

Související úlohy

Připojení aplikací klienta produktu IBM MQ MQI ke správcům front

Související odkazy

ZOBRAZIT CHLAUTH

NASTAVIT CHLAUTH

Který typ komunikace použít

Různé platformy podporují různé komunikační protokoly. Volba přenosového protokolu závisí na vaší kombinaci klientských a serverových platforem produktu WebSphere MQ MQI.

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 klienty WebSphere MQ MQI může být užitečné používat alternativní kanály MQI s použitím různých přenosových protokolů.

Volba přenosového protokolu závisí také na konkrétní kombinaci klientských a serverových platforem produktu WebSphere MQ . Možné kombinace jsou uvedeny v následující tabulce.

Tabulka 14. Přenosové protokoly-kombinace klientských a serverových platforem WebSphere MQ

Přenosový protokol	**Klient WebSphere MQ MQI**	**Server WebSphere MQ**
Protokol TCP/IP	Systémy UNIX Windows	Systémy UNIX Windows
LU 6.2	Systémy UNIX[1] Windows	Systémy UNIX[1] Windows
NetBIOS	Windows	Windows
SPX	Windows	Windows

Poznámka:

1. Kromě Linux (platformy POWER)

Související pojmy

“Definování připojení TCP na systému Windows” na stránce 82

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 UNIX and Linux” na stránce 91

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

“Definování připojení LU 6.2 na systému Windows” na stránce 83

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

“Definování připojení LU 6.2 na serveru UNIX and Linux” na stránce 94

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

“Definování připojení NetBIOS v systému Windows” na stránce 85
Produkt WebSphere MQ používá tři typy prostředků NetBIOS při vytváření připojení NetBIOS k jinému produktu WebSphere MQ : relace, příkazy a názvy. Každý z těchto prostředků má limit, který je standardně nastaven buď standardně, nebo volbou během instalace NetBIOS.

“Definování připojení SPX v systému Windows” na stránce 88
Připojení SPX se vztahuje pouze na klienta a server se systémem Windows XP a Windows 2003 Server.

Související odkazy

“limity připojení TCP/IP” na stránce 99
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 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 WebSphere 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 15. 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 UNIX and Linux nebo `amqerr0n.log` v podadresáři chyb instalace klienta IBM WebSphere 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 nebo SPX

Připojení NetBIOS a SPX platí pouze pro systémy Windows .

Připojení NetBIOS se vztahuje pouze na klienta a server se systémem Windows. Viz Definování připojení NetBIOS.

Připojení SPX se vztahuje pouze na klienta a server se systémem Windows XP nebo Windows 2003 Server. Viz Definování připojení SPX.

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 XA, jako je CICS a Tuxedo.

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

WebSphere Application Server
Dřívější verze produktu WebSphere MQ podporovaly produkt WebSphere Application Server verze 4 nebo verze 5 a vyžadovaly, abyste provedli určité konfigurační úlohy pro použití rozšířeného transakčního klienta. Produkt WebSphere Application Server verze 6 a vyšší zahrnuje poskytovatele systému zpráv produktu WebSphere MQ , takže nemusíte používat rozšířeného transakčního klienta.

Související pojmy

“Konfigurace správců transakcí s podporou standardu XA” na stránce 100
Nejprve nakonfigurujte základního klienta WebSphere MQ a poté nakonfigurujte rozšířenou transakční funkci s použitím informací v těchto tématech.

“ Microsoft Transaction Server.” na stránce 108
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 WebSphere MQ a poté 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 konfigurovat rozšířeného transakčního klienta, je třeba nejprve konfigurovat základního klienta WebSphere MQ , jak je popsáno v tématu Instalace klienta IBM WebSphere MQ . Pomocí informací v této sekci můžete nakonfigurovat rozšířenou transakční funkci pro správce transakcí vyhovující specifikaci XA, jako např. 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 WebSphere MQ , může být souběžně připojena k více než jednomu správci front 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 konfigurovat 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_info*na 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 102.

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 105.

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 CICS” na stránce 106
- “Konfigurace rozšířeného transakčního klienta pro Tuxedo” na stránce 108

Související pojmy

“Parametry CHANNEL, TRPTYPE, CONNAME a QMNAME řetězce xa_open” na stránce 103
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 105
Volání xa_open selhává za určitých okolností.

Související úlohy

"Použití rozšířeného transakčního klienta s kanály SSL" na stránce 106
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 104
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 transakčního zpracování" na stránce 105
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.

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, adresa uzlu 6bajtového 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 systému z/OS , 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.

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.

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 klient aplikace připojuje ke správci front systému 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.

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

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.

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 16 na stránce 104 , kde jsou převzaty hodnoty parametru AXLIB.

Tabulka 16. 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 jakékoliv 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.

Pokud budete někdy potřebovat změnit jakékoli informace o konfiguraci, musíte se ujistit, že všechny nedokončené jednotky práce byly vyřešeny před provedením změn. 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 17 na stránce 105.

Tabulka 17. Knihovny WebSphere MQ obsahující struktury přepínačů XA

Platforma	**Knihovna obsahující struktury přepínačů XA**
AIX HP-UX Linux Solaris	*MQ_INSTALLATION_PATH*/lib/libmqcxa
systémy Windows	*MQ_INSTALLATION_PATH*\bin\mqcxa.dll [1]
Produkt *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, do kterého je produkt WebSphere MQ nainstalován.	

Název správce prostředků produktu WebSphere MQ v každé struktuře přepínače je MQSeries_XA_RMI, ale řada správců front může sdílet stejnou strukturu přepínačů.

Související pojmy

“Dynamická registrace a rozšířené transakční zpracování” na stránce 106
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 MQCONNX 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 systému 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 CICS
Rozšířený transakční klient pro použití produktem CICS nakonfigurujete tak, že přidáte definici prostředku XAD do oblasti CICS .

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

- Řetězec xa_open
- Úplný název úplné cesty k souboru načtení přepínače

Jeden soubor pro načtení přepínače je dodáván pro použití produktem CICS na každé z následujících platforem: AIX, HP-UX, Solaris a Windows .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 18 na stránce 107 .

Tabulka 18. 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]
Produkt *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, do kterého je produkt WebSphere MQ nainstalován.	

Zde je příklad definice prostředku XAD pro systémy Windows :

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

For more information about adding an XAD resource definition to a CICS region, see the *CICS Administration Reference* and the *Příručka administrace produktu CICS* for your platform.

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

- Můžete přidat pouze jednu definici prostředku XAD pro produkt WebSphere MQ do oblasti CICS . Tento znamená, že k oblasti může být přidružen pouze jeden správce front a všechny aplikace CICS , které běží v regionu, se mohou připojit pouze k tomuto správci front. Chcete-li spustit aplikace CICS , které se připojují k jinému správci front, musíte 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 klienta produktu WebSphere MQ MQI, které byly později zpracovány 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 připojení serveru MCA pro připojení k serveru, `cics`. Under certain circumstances, the queue manager uses this user ID for authority checks when the server connection MCA subsequently attempts to access the queue manager resources on behalf of a client application. Pokud se toto ID uživatele používá pro kontroly 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 produktu CICS , které jsou dodávány pro použití v klientských systémech WebSphere MQ , jsou uvedeny v seznamu Tabulka 19 na stránce 107. Tyto uživatelské procedury se konfigurují stejným způsobem, jakým konfigurujete příslušné uživatelské procedury pro systémy WebSphere MQ . Pro tyto informace se proto podívejte na téma Povolení uživatelských procedur CICS.

Tabulka 19. Ukončení ukončení úlohy CICS		
Platforma	**Zdroj**	**Knihovna**
AIX HP-UX Linux Solaris	amqzscgx.c	amqczscg

Tabulka 19. Ukončení ukončení úlohy CICS (pokračování)		
Platforma	**Zdroj**	**Knihovna**
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 systému AIX, HP-UXa Solaris je název souboru ubbstxcx.cfg a na systémech Windows je to název souboru `ubbstxcn.cfg`.
- V položce pro správce front v tabulce správce prostředků produktu Tuxedo:
  - udataobj/RM (AIX, HP-UXa 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 Transaction 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 předání aplikace WebSphere MQ na klientském počítači klienta WebSphere MQ MQI ke kanálu.

Tyto dvě metody jsou podrobně popsány:

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

   Toto platí pro libovolnou kombinaci klientských a serverových platforem produktu WebSphere MQ MQI. 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 110 .
2. Vytvořte obě definice kanálů na počítači serveru.

   Tuto metodu použijte v případě, že nastavujete více kanálů a klientské počítače WebSphere MQ MQI ve stejnou dobu.

   Podrobné informace o způsobu použití této metody naleznete v příručce “Vytvoření připojení k serveru a připojení klienta na serveru” na stránce 113 .

Automaticky definované kanály

Produkty WebSphere 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 tomto správci front nalézt příslušnou definici připojení serveru, produkt WebSphere MQ ji vytvoří automaticky a přidá ji ke správci 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).

Další informace o automatickém vytváření definic kanálů naleznete v tématu Automatická definice přijímacích kanálů a kanálů připojení serveru.

Související pojmy

“Automaticky definované kanály” na stránce 110
Produkty WebSphere MQ na platformách jiných než z/OS zahrnují funkci, která může automaticky vytvořit definici kanálu na serveru, pokud taková neexistuje.

“Kanály definované uživatelem” na stránce 110
Pokud server automaticky nedefinuje kanály, existují dva způsoby vytvoření definic kanálů a předání aplikace WebSphere MQ na klientském počítači klienta WebSphere MQ MQI ke kanálu.

“Řídicí funkce kanálu” na stránce 52
Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

Automaticky definované kanály

Produkty WebSphere 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 tomto správci front nalézt příslušnou definici připojení serveru, produkt WebSphere MQ ji vytvoří automaticky a přidá ji ke správci 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).

Kanály definované uživatelem

Pokud server automaticky nedefinuje kanály, existují dva způsoby vytvoření definic kanálů a předání aplikace WebSphere MQ na klientském počítači klienta WebSphere MQ MQI ke kanálu.

Tyto dvě metody jsou podrobně popsány:

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

   Toto platí pro libovolnou kombinaci klientských a serverových platforem produktu WebSphere MQ MQI. 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 110 .
2. Vytvořte obě definice kanálů na počítači serveru.

   Tuto metodu použijte v případě, že nastavujete více kanálů a klientské počítače WebSphere MQ MQI ve stejnou dobu.

   Podrobné informace o způsobu použití této metody naleznete v příručce “Vytvoření připojení k serveru a připojení klienta na serveru” na stránce 113 .

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 WebSphere MQ Script (MQSC), programovatelných formátů příkazů (PCF) nebo Průzkumníka IBM WebSphere MQ definovat kanál připojení serveru na počítači serveru.

Vzhledem k tomu, že příkazy MQSC nejsou k dispozici v počítači, ve kterém byl produkt WebSphere MQ nainstalován pouze jako klient WebSphere MQ MQI, musíte na klientském počítači použít různé způsoby definování kanálu připojení klienta.

Související pojmy

“Vytvoření kanálu připojení klienta na klientu IBM WebSphere MQ MQI” na stránce 111
Na pracovní stanici klienta můžete definovat kanál připojení klienta pomocí MQSERVER nebo pomocí struktury MQCNO na volání MQCONNX.

Související úlohy

“Definování kanálu připojení serveru na serveru” na stránce 110
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:

```
crtmqm QM1
```

b) Spusťte správce front:

```
strmqm 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 klientu IBM WebSphere MQ MQI

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

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 definici jednoduchého kanálu na serveru Windows následujícím způsobem:

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

- Určete jednoduchou definici kanálu na systémech UNIX and Linux následujícím způsobem:

```
export MQSERVER=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 klienta IBM WebSphere MQ MQI:
  - LU62
  - TCP
  - NETBIOS
  - SPX

Poznámka: Na systémech UNIX and 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).

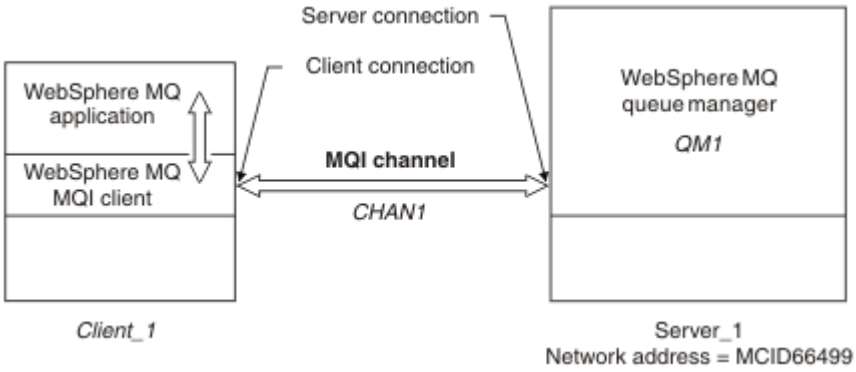
Například v systému Windows:

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

nebo, v systémech UNIX and Linux :

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

Poznámka: Informace o změně čísla portu TCP/IP naleznete v části “SERVER MQSERVER” na stránce 145.



Obrázek 17. Jednoduchá definice kanálu

Některé další příklady definic jednoduchého kanálu jsou:

- V systému Windows:

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

- Na systémech UNIX and Linux :

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

kde B0X99 je LU 6.2 ConnectionName.

Na klientovi IBM WebSphere MQ MQI se 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* naleznete v tématu “SERVER MQSERVER” na stránce 145.

Použití struktury MQCNO u volání MQCONNX

Aplikace klienta IBM WebSphere MQ MQI může prostřednictvím struktury voleb připojení, MQCNO, ve volání **MQCONNX** odkazovat 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 **MQCONNX** .

Další informace o strukturách MQCNO, MQCD a MQSCO naleznete v části MQCNO, MQCDa MQSCO.

Poznámka: Ukázkový program pro MQCONNX se nazývá **amqscnxc**. Jiný ukázkový program s názvem **amqsssl c** 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 lze pomocí příkazů WebSphere MQ Script (MQSC), programmable command format (PCF) nebo Průzkumníka IBM WebSphere MQ definovat kanál připojení serveru na počítači serveru.

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 113
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 115
Vytvořte definici kanálu připojení serveru pro daného správce front.

“Definování kanálu pro připojení klienta na serveru” na stránce 116
Při definování kanálu připojení serveru je nyní definován příslušný kanál připojení klienta.

“Přístup k definicím kanálu připojení klienta” na stránce 117
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 nečte soubor CCDT.

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

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.

Platformy jiné 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:

- Linux UNIX Na systémech UNIX and Linux :

  ```
  /prefix/qmgrs/QUEUEMANAGERNAME/@ipcc
  ```

  Název adresáře, na který se odkazuje *QUEUEMANAGERNAME* , je na systémech UNIX and 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 V systému Windows:

  ```
  MQ_INSTALLATION_PATH\data\qmgrs\QUEUEMANAGERNAME\@ipcc
  ```

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

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.
- Použije 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 143
`MQCHLLIB` uvádí cestu k adresáři se souborem obsahujícím tabulku definic kanálů klienta (CCDT). Soubor je vytvořen na serveru, ale lze jej zkopírovat do pracovní stanice klienta WebSphere MQ MQI.

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 WebSphere MQ na další. V důsledku toho může klient IBM WebSphere MQ MQI 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.

Klient MQI verze 7.1 IBM WebSphere MQ může použít tabulku definic kanálů klienta, která byla připravena správcem front verze 6.0 . Ale klient verze 6.0 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, produkt IBM WebSphere 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 WebSphere MQ také v adresáři Active Directory. Když klient IBM WebSphere MQ určí, jak se připojit k serveru, hledá odpovídající definici objektu kanálu připojení klienta pomocí následujícího pořadí vyhledávání:

1. Datová struktura MQCONNX 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 WebSphere 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')
   ```

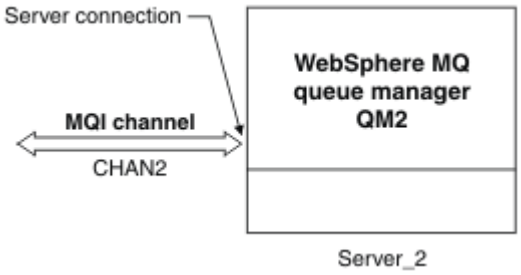
2. Pomocí následujícího příkazu můžete povolit přístup pro příchozí připojení k vašemu správci front:

   ```
   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 18. 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 (CONNAME). 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 WebSphere 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) +
   CONNAME(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:

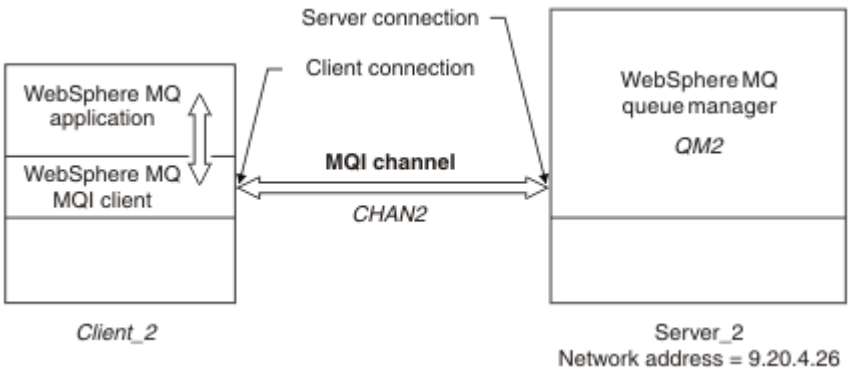
   ```
   SET CHLAUTH(CHAN2) TYPE(ADDRESSMAP)  ADDRESS('IP-address') MCAUSER('userid')
   ```

   - 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

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 uloženy v produktu z/OS, naleznete v tématu “Tabulka definic kanálů klienta” na stránce 113.



Obrázek 19. 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 133.
   b) Volitelné: Použijte proměnné prostředí MQCHLLIB a MQCHLTAB.

      Proměnné prostředí můžete nastavit například zadáním příkazu:

      - V systémech HP Integrity NonStop Servera UNIX and Linux :

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

      kde *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, do kterého je produkt WebSphere MQ nainstalován.
   c) Volitelné: Pouze v systému Windows použijte řídicí příkaz **setmqscp** k publikování definic kanálů připojení klienta v Active Directory .

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

Programy pro ukončení kanálů pro kanály MQI

Na systémech UNIX, Linux a Windows jsou k dispozici tři typy uživatelské procedury kanálu pro klientské prostředí WebSphere MQ MQI.

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 WebSphere MQ, ale možná budete chtít použít jinou techniku komprese)
- šifrování a dešifrování uživatelských dat (tato funkčnost je poskytována jako součást produktu WebSphere MQ, ale možná budete chtít použít jinou techniku šifrování)
- Žurnálování každé odeslané a přijaté zprávy

Pomocí uživatelské procedury zabezpečení můžete zajistit, aby byl klient a server WebSphere MQ správně identifikován a aby mohl řídit přístup.

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, použije 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 119
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.

Uživatelské procedury, uživatelské procedury rozhraní API a instalovatelné služby produktu WebSphere MQ

Související úlohy

Rozšíření zařízení správce front

Související odkazy

“Cesta k východům” na stránce 118
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 120
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.

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 klienta WebSphere MQ MQI přidán do vašeho systému 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 ClientExitje 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 20 na stránce 120 ilustruje použití bezpečnostních procedur v připojení klienta pomocí správce oprávnění k objektu WebSphere 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.

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

Poznámka: Uživatelské aplikace zabezpečení vytvořené před vydáním produktu WebSphere 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 20. Identifikace volání rozhraní API

Volání rozhraní API	**Hodnota bajtu 10 pro požadavek**	**Hodnota bajtu 10 pro odpověď**
MQCONN “1” na stránce 121,“2” na stránce 121	X'81 '.	X "91"
MQDISC “1” na stránce 121	X'82 '	X "92"

Tabulka 20. Identifikace volání rozhraní API (pokračování)

Volání rozhraní API	**Hodnota bajtu 10 pro požadavek**	**Hodnota bajtu 10 pro odpověď**
MQOPEN “3” na stránce 121	X'83 '	X "93"
MQCLOSE	X'84 '	X "94"
MQGET “4” na stránce 121	X'85 '	X "95"
MQPUT “4” na stránce 121	X'86 '	X "96"
Požadavek MQPUT1 “4” na stránce 121	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.

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.

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. Připojíte se ke skupině pomocí generického rozhraní, když se nechcete připojit ke specifickému správci front v rámci skupiny sdílení front.

Generické rozhraní může být název skupiny WLM/DNS nebo generický název prostředku VTAM , nebo jiné společné rozhraní ke skupině 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) +
MCAUSER(' ') QSGDISP(GROUP)
```

Definice kanálů na serveru jsou uloženy ve sdíleném úložišti 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) +
CONNAME(WLM/DNS groupname) 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 vlastněných touto skupinou.

Související pojmy

“Vytvoření definic kanálů” na stránce 122
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.

Vytvoření definic kanálů

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) +
MCAUSER(' ') QSGDISP(GROUP)
```

Definice kanálů na serveru jsou uloženy ve sdíleném úložišti 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) +
```

```
CONNAME(WLM/DNS groupname) 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 vlastněných touto skupinou.

Konfigurace klienta pomocí konfiguračního souboru

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

Server IBM WebSphere MQ MQI client se konfiguruje pomocí textového souboru, podobně jako u konfiguračního souboru správce front qm.ini, který se používá na platformách UNIX and Linux . Soubor obsahuje řadu oddílů, z nichž každý obsahuje řadu řádků ve formátu **attribute-name**=*hodnota* .

V této dokumentaci je tento soubor označován jako *konfigurační soubor klientaWebSphere MQ MQI*; jeho název souboru je obecně mqclient.ini, ale můžete jej zadat i jiným názvem. Konfigurační informace v tomto souboru platí pro všechny platformy a pro klienty používající rozhraní MQI, IBM WebSphere MQ classes for Java, IBM WebSphere MQ classes for JMS, IBM WebSphere MQ classes for .NETa XMS.

Ačkoli se atributy v konfiguračním souboru IBM WebSphere MQ MQI client vztahují na většinu klientů IBM WebSphere MQ , existují některé atributy, které nejsou čteny spravovanými klienty .NET a XMS .NET , nebo klienty, kteří používají buď IBM WebSphere MQ classes for Java nebo IBM WebSphere MQ classes for JMS. Další informace viz “Kteří klienti IBM WebSphere MQ mohou číst každý atribut” na stránce 125.

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 taková proměnná prostředí odpovídá ekvivalentní hodnotě v konfiguračním souboru klienta, proměnná prostředí přepíše hodnotu konfiguračního souboru klienta.

V případě klientské aplikace pomocí produktu IBM WebSphere MQ classes for JMSmůžete také přepsat konfigurační soubor klienta následujícími způsoby:

- nastavení vlastností v konfiguračním souboru JMS
- nastavení vlastností systému Java, které také přepíše konfigurační soubor JMS

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

Povšimněte si, že pomocí konfiguračního souboru klienta nelze nastavit více připojení kanálu.

Příklad konfiguračního souboru klienta

```
#* Module Name: mqclient.ini                                          *#
#* Type       : WebSphere 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

“Umístění konfiguračního souboru klienta” na stránce 124
Konfigurační soubor klienta IBM WebSphere MQ MQI lze uložit v několika umístěních.

“stanza CHANNELS konfiguračního souboru klienta” na stránce 133
Použijte sekci CHANNELS k uvedení informací o kanálech klienta.

“stanza cesty ClientExitkonfiguračního souboru klienta” na stránce 135
Pomocí oddílu Cesta ClientExiturčete výchozí umístění kanálů kanálu na straně klienta.

“Stanzy LU62, NETBIOS a SPX v konfiguračním souboru klienta” na stránce 135
Pouze na systémech Windows použijte tyto sekce k uvedení konfiguračních parametrů pro zadané síťové protokoly.

“stanza MessageBuffer konfiguračního souboru klienta” na stránce 136
Použijte sekci MessageBuffer k uvedení informací o vyrovnávacích pamětech zpráv.

“stanza SSL konfiguračního souboru klienta” na stránce 138
Použijte sekci SSL k uvedení informací o použití SSL nebo TLS.

“Sekce TCP konfiguračního souboru klienta” na stránce 140
stanzu TCP použijte k uvedení konfiguračních parametrů síťového protokolu TCP.

“Použití proměnných prostředí produktu WebSphere MQ” na stránce 141
Tento oddíl popisuje proměnné prostředí, které lze použít s klientskými aplikacemi WebSphere MQ MQI.

“Změna konfiguračních informací správce front” na stránce 418
Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro produkt WebSphere MQ.

Umístění konfiguračního souboru klienta

Konfigurační soubor klienta IBM WebSphere MQ MQI lze uložit v několika umístěních.

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

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 C, .NET a XMS podporují pouze protokol `file:` ; pokud řetězec adresy URL nezačíná řetězcem `protocol:` , předpokládá se protokol `file:` .
   - Chcete-li povolit prostředí JRE Java 1.4.2 , která nepodporuje čtení proměnných prostředí, lze proměnnou prostředí MQCLNTCF přepsat pomocí vlastností systému Java MQCLNTCF.

2. Soubor s názvem `mqclient.ini` v současném pracovním adresáři aplikace.
3. Soubor nazvaný `mqclient.ini` v datovém adresáři IBM WebSphere MQ pro systémy Windows, systémy UNIX and Linux .

   Všimněte si následujícího:

   - Datový adresář produktu IBM WebSphere MQ neexistuje na určitých platformách, například IBM i a z/OS, nebo v případech, kdy byl klient dodán s jiným produktem.
   - Na systémech UNIX and Linux je to adresář `/var/mqm` .
   - Na platformách Windows nakonfigurujte proměnnou prostředí MQ_FILE_PATH během instalace tak, aby ukazovala na datový adresář. Obvykle je `C:\Program Files\IBM\WebSphere MQ`
   - Chcete-li povolit prostředí JRE Java 1.4.2 , která nepodporují čtení proměnných prostředí, můžete proměnnou prostředí MQ_FILE_PATH ručně potlačit proměnnou prostředí MQ_FILE_PATH Java System Property.
4. Soubor s názvem `mqclient.ini` ve standardním adresáři, který je vhodný pro platformu a je přístupný uživatelům:
   - Pro všechny klienty prostředí Java se jedná o hodnotu systémové vlastnosti Java systému `user.home` .
   - Pro klienty jazyka C na platformách UNIX and Linux se jedná o hodnotu proměnné prostředí HOME.
   - Pro klienty jazyka C v systému Windows se jedná o zřetězené hodnoty proměnných prostředí HOMEDRIVE a HOMEPATH.

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

Kteří klienti IBM WebSphere MQ mohou číst každý atribut

Většina atributů v konfiguračním souboru IBM WebSphere 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 WebSphere MQ classes for Java , nebo IBM WebSphere MQ classes for JMS.

Tabulka 21. 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						
CCSID	Kódované číslo znakové sady, které má být použito.	Ano	Ne	Ne	Ano	Ano
ChannelDefinition	Cesta k adresáři se souborem obsahujícím tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano

Tabulka 21. 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**
ChannelDefinition	Název souboru obsahujícího tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano
ReconDelay	Administrativní volba pro konfiguraci prodlevy opětného připojení pro klientské programy, které se mohou automaticky znovu připojit.	Ano	Ne	Ano	Ano	Ano
DefRecon	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
MQReconnectTimeout	Časový limit v sekundách, který se má znovu připojit ke klientovi.	Ano	Ne	Ne	Ano	Ne

Tabulka 21. 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**
ParametryServerConnectionParms	Umístění serveru IBM WebSphere MQ a komunikační metoda, která má být použita.	Ano	Ne	Ne	Ano	Ano
Put1DefaultAlwaysSync	Řídí chování volání funkce MQPUT1 s volbou `MQPMO_RESPONSE_AS_Q_DEF`.	Ano	Ano	Ano	Ano	Ano
ClientExit-stanza cesty						
ExitsDefaultPath	Určuje umístění 32bitového kanálu pro klienty.	Ano	Ne	Ne	Ano	Ano
ExitsDefaultPath64	Určuje umístění 64bitových kanálů kanálů pro klienty.	Ano	Ne	Ne	Ano	Ano
JavaExitsClassPath	Hodnoty, které mají být přidány do cesty ke třídě při spuštění uživatelské procedury produktu Java .	Ne	Ano	Ano	Ne	Ne
stanzaMessageBuffer						

Tabulka 21. 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**
MaximumSize	Velikost vyrovnávací paměti dopředného čtení v kilobajtech, v rozsahu od 1 do 999 999.	Ano	Ano	Ano	Ano	Ano
PurgeTime	Interval, v sekundách, po jehož uplynutí jsou vyprázdněny zprávy ponechané ve vyrovnávací paměti dopředného čtení.	Ano	Ano	Ano	Ano	Ano
UpdatePercentage	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
Sekce SSL						

Tabulka 21. 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**
CDPCheckExtensions	Určuje, zda se kanály SSL nebo TLS v tomto správci front pokusí zkontrolovat servery CDP, které jsou pojmenované v rozšířeních certifikátu bodu CrlDistribution.	Ano	Ne	Ne	Ne	Ne
CertificateLabel	Jmenovka certifikátu pro definici kanálu.	Ano	Ne	Ne	Ne	Ne
CertificateVal	Určuje typ použitého ověření certifikátu.	Ano	Ne	Ne	Ne	Ne
ClientRevocation-kontroly	Určuje, jak je kontrola odvolání certifikátů konfigurována, pokud volání connect klienta používá kanál SSL/TLS.	Ano	Ne	Ne	Ne	Ne
EncryptionPolicySuiteB	Určuje, zda kanál používá šifrování vyhovující standardu Suite-B a jaká úroveň síly se má použít.	Ano	Ne	Ne	Ne	Ne

Tabulka 21. 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**
OCSPAuthentication	Definuje chování produktu IBM WebSphere 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 WebSphere MQ funguje na rozšíření certifikátu AuthorityInfoAccess.	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 21. 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**
SSLFipsRequired	Určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, je-li šifrování prováděno v produktu IBM WebSphere MQ.	Ano	Ne	Ne	Ne	Ne
SSLHTTPProxyName	Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použít 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 21. 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**
ClntRcvBuffSize	Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.	Ano	Ano	Ano	Ano	Ano
ClntSndBuffSize	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
Časový limit připojení	Počet sekund před pokusem o připojení k vypršení časového limitu soketu.	Ano	Ano	Ano	Ne	Ne
IPAddressVersion	Určuje protokol IP, který má být použit pro připojení kanálu.	Ano	Ne	Ne	Ano	Ano

Tabulka 21. 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 produkt 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.

Ve stanze CHANNELS mohou být zahrnuty následující atributy:

CCSID=*číslo*
Kódované číslo znakové sady, které má být použito.

Číslo CCSID je ekvivalentní parametru prostředí MQCCSID.

ChannelDefinitionDirectory=*cesta*
Cesta k adresáři se souborem obsahujícím tabulku definic kanálů klienta.

V systému Windows je výchozím nastavením instalační adresář produktu IBM WebSphere MQ , zpravidla `C:\Program Files\IBM\WebSphere MQ`. U systémů UNIX and 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.

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. 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.

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.

Automatické opětovné připojení klienta není podporováno třídami IBM WebSphere MQ pro jazyk Java.

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 22. 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_RECONNECT	MQCNO_RECONNECT_Q_MGR	MQCNO_RECONNECT_AS_DEF	MQCNO_RECONNECT_DISABLED
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).

Klienti produktu IBM WebSphere MQ classes for XMS .NET mohou určit časový limit opakovaného připojení pomocí vlastnosti XMSC.WMQ_CLIENT_RECONNECT_TIMEOUT. Výchozí hodnota této vlastnosti je 1800 sekund (30 minut).

ServerConnectionParms
Parametry ServerConnectionParms jsou ekvivalentní parametru prostředí MQSERVER a určují umístění serveru IBM WebSphere MQ a způsobu komunikace, který má být použit. Atribut Parametry parametru ServerConnectionParams definuje pouze jednoduchý kanál; nelze jej 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 dopředné lomítko ("/"). 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.

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 .

stanza cesty ClientExitkonfiguračního souboru klienta

Pomocí oddílu Cesta ClientExiturčete výchozí umístění kanálů kanálu na straně klienta.

Následující atributy mohou být zahrnuty do stanzy ClientExitPath:

ExitsDefaultPath=*řetězec*
Určuje umístění 32bitového kanálu pro klienty.

ExitsDefaultPath64=*řetězec*
Určuje umístění 64bitových kanálů kanálů pro klienty.

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

V konfiguračním souboru služby JMS má název JavaExitsClassPath standard com.ibm.mq.cfg. a tento úplný název je také použit ve vlastnosti systému Websphere MQ V7.0 . Ve verzi 6.0 byl tento atribut zadán s použitím systémové vlastnosti com.ibm.mq.exitClasspath, která byla dokumentována v souboru Readme verze 6.0 . Použití objektu com.ibm.mq.exitClasspath bylo zamítnuto. Pokud jsou přítomny obě volby JavaExitsClassPath a exitClasspath , je JavaExitsClassPath poctěn. Je-li k dispozici pouze použití exitClasspath , je v produktu Websphere MQ V7.0stále dodržován.

Stanzy LU62, NETBIOS a SPX v konfiguračním souboru klienta

Pouze na systémech Windows použijte tyto sekce k uvedení konfiguračních parametrů pro zadané síťové protokoly.

LU62

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

Library1=*DLLName*|WCPIC32
Název knihovny APPC DLL.

Library2=*DLLName*|WCPIC32
Stejné jako Library1, používá se, pokud je kód uložen ve dvou samostatných knihovnách.

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

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.

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.

Do sekce MessageBuffer mohou být zahrnuty následující atributy:

MaximumSize=*celé_číslo*|1
Velikost vyrovnávací paměti dopředného čtení v kilobajtech, v rozsahu od 1 do 999 999.

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.

Pokud klientská aplikace vybírá zprávy založené na hodnotě MsgId nebo CorrelId , může dojít k tomu, 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 od 1 do 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.

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*. Hodnota *n* se vynuluje pokaždé, když se odešle nový požadavek na server.

Prahová hodnota T se vypočítá takto:

```
T = Upper - Lower
```

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

Dolní je menší než velká hodnota a je určen atributem *UpdatePercentage* . Tento atribut je číslo v rozsahu od 1 do 100 a má výchozí hodnotu 20. Nižší hodnota se vypočítá takto:

```
Lower = Upper x 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 MQGET nespotřebuje n bajtů.

Použití výpočtu

```
T = Upper - Lower
```

T je (100-20) = 80 Kb.

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

Příklad 2:

Atributy MaximumSize mají 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 MQGET nespotřebuje n bajtů.

Použití výpočtu

```
T = Upper - 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 odesílaných 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 SSL konfiguračního souboru klienta

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

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 rozšířeních certifikátu bodu CrlDistributionPoint.

Tento atribut může mít následující hodnoty:

- ANO: Kanály SSL nebo TLS se snaží zkontrolovat servery CDP za účelem určení, zda je digitální certifikát odvolán.
- NO: 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 .

CertificateValPolicy=*řetězec*
Určuje typ použitého ověření certifikátu.

ANY
Použijte jakoukoli zásadu ověření platnosti certifikátu podporovanou základní zabezpečenou knihovnou soketů. 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.

Windows 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 nenezdaří.

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. Možné hodnoty jsou:

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 WebSphere MQ , je-li protokol OCSP povolen a kontrola odvolání OCSP není schopna určit stav odvolání certifikátu. Existují tři možné 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 je povoleno pokračovat

OCSPCheckExtensions=YES|NO
Určuje, zda produkt WebSphere MQ pracuje s rozšířeními certifikátu AuthorityInfoAccess. Je-li hodnota nastavena na NO, produkt WebSphere 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.

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;passw0rd;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. Hodnota tohoto parametru je buď:

SYMMETRIC_CIPHER_VYPNUTO
Nepřistupovat 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, pokud je šifrování prováděno v produktu WebSphere MQ. Je-li konfigurován kryptografický hardware, použité šifrovací moduly jsou moduly, které poskytuje 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. Na platformách HP-UX PA-RISC a Sun Solaris SPARC a pro 32bitové klienty v systému AIXmůže 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 odpovídacího 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.

SSLKeyResetCount=*celé_číslo*|0
Počet nezašifrovaných bajtů odeslaných a přijatých na kanál SSL nebo TLS, než je znovu vyjednán tajný klíč.

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.

Následující atributy mohou být zahrnuty do stanzy TCP:

ClntRcvBuffSize=*číslo*|32768
Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta. Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, na rozdíl od velikosti vyrovnávací paměti, které byly opraveny produktem WebSphere MQ.

ClntSndBuffSize=*číslo*|32768
Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta. Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, na rozdíl od velikosti vyrovnávací paměti, které byly opraveny produktem WebSphere MQ.

Connect_Timeout=*číslo*
Počet sekund před pokusem o připojení k vypršení časového limitu soketu; výchozí hodnota je 0, pokud nebyl kanál konfigurován s nulovým váhami kanálu klienta, který není nulový, v tom případě je výchozí hodnota 5.

IPAddressVersion=MQIPADDR_IPV4|MQIPADDR_IPV6
Určuje protokol IP, který má být použit pro připojení kanálu.

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.

Windows **Library1=*DLLName*|_WSOCK32**
(Pouze pro systém Windows) Název knihovny DLL soketů TCP/IP.

stanza TMF a TMF/Gateway

Produkt IBM WebSphere MQ poskytuje TMF/Gateway, která je spuštěna v prostředí Pathway. Použijte sekce TMF a TMF/Gateway k uvedení požadovaných konfiguračních parametrů pro klienta IBM WebSphere MQ pro produkt HP Integrity NonStop Server pro komunikaci s TMF/Gateway.

Chcete-li použít TMF, pak musíte definovat sekci TMF a jednu sekci TmfGateway pro každého správce front, se kterým komunikujete. Všechny hodnoty jsou odvozeny z vaší konfigurace.

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
```

Použití proměnných prostředí produktu WebSphere MQ

Tento oddíl popisuje proměnné prostředí, které lze použít s klientskými aplikacemi WebSphere MQ MQI.

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

WebSphere MQ používá výchozí hodnoty pro ty proměnné, které jste nenastavili.

Příkazy jsou k dispozici na všech klientských platformách produktu WebSphere MQ MQI, není-li uvedeno jinak.

Pro každou proměnnou prostředí použijte příkaz příslušný pro vaši platformu k zobrazení aktuálního nastavení nebo k resetování hodnoty proměnné.

Příklad:

Nastavení nebo resetování hodnoty proměnné prostředí		
Efekt	**Příkaz**	
	Windows	**Systémy UNIX and Linux**
Odebere proměnnou.	NASTAVIT PARAMETR MQSERVER=	unset MQSERVER
Zobrazí aktuální nastavení	NASTAVIT PŘÍKAZ MQSERVER	echo $MQSERVER
Zobrazí všechny proměnné prostředí pro relaci	set	set

Informace o jednotlivých proměnných naleznete v následujících dílčích tématech:

Související pojmy

“Konfigurace klienta pomocí konfiguračního souboru” na stránce 123
Nakonfigurujte klienty pomocí atributů v textovém souboru. Tyto atributy mohou být přepsány proměnnými prostředí nebo jinými způsoby specifickými pro platformu.

Související odkazy

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 systémy Windows:

```
SET MQCCSID=number
```

- Pro systémy UNIX and Linux :

```
export MQCCSID=number
```

MQCERTVPOL

Modul MQCERTVPOL určuje použitou zásadu ověření certifikátu.

Další informace o zásadách ověření platnosti certifikátů v produktu WebSphere MQnaleznete v tématu Zásady ověření platnosti certifikátů v produktu WebSphere 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 soketů.

RFC5280
Používejte pouze ověření certifikátu, které je v souladu s normou RFC 5280.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Pro systémy Windows:

```
SET MQCERTVPOL=value
```

- Pro systémy UNIX and Linux :

```
export MQCERTVPOL=value
```

MQCHLLIB

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

Není-li parametr MQCHLLIB nastaven, je cesta pro klienta standardně nastavena na:

- Windows Pro systémy Windows: *MQ_INSTALLATION_PATH*
- Linux UNIX Pro systémy UNIX and Linux : /var/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.

- Windows Pro systémy Windows: *datapath*\@ipcc
- Linux UNIX Pro systémy UNIX a Linux: *datapath*/@ipcc

Nebo:

- Windows Pro systémy Windows: *MQ_INSTALLATION_PATH*\data\qmgrs*qmgrname*\@ipcc
- Linux UNIX Pro systémy UNIX and Linux : /prefix/qmgrs/*qmgrname*/@ipcc

kde:

- *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM WebSphere 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 UNIX a Linux.
- *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 mqs.ini v systému UNIXa Linuxa v registru systému Windows .

Notes:

1. Je-li nastavena hodnota, MQCHLLIB potlačí cestu použitou k umístění tabulky CCDT.
2. Proměnné prostředí, jako např. MQCHLLIB, mohou být vymezeny na proces nebo úlohu nebo celosystémově specifické, v závislosti na platformě.
3. 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** .
4. 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.

5. 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.
6. 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.
7. Ostatní příkazy, které aktualizují CCDT, upravují pouze kanály připojení klienta se stejným názvem kanálu. Ostatní kanály připojení klienta v souboru se nezmění.
8. Cesta pro MQCHLLIB nevyžaduje uvozovky.

Příklady

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Windows Pro systémy Windows:

```
SET MQCHLLIB=pathname
```

  Příklad:

```
SET MQCHLLIB=C:\wmqtest
```

- Linux UNIX Pro systémy UNIX and Linux :

```
export MQCHLLIB=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 113.

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- V systému Windows:

```
SET MQCHLTAB=filename
```

- Na systémech UNIX and Linux :

```
export MQCHLTAB=filename
```

Příklad:

```
SET MQCHLTAB=ccdf1.tab
```

Stejným způsobem jako pro klienta určuje proměnná prostředí MQCHLTAB na serveru název tabulky definic kanálů klienta.

MQIPADRV

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 hodnota "MQIPADDR_IPV4".

Chcete-li nastavit tuto proměnnou, použijte jeden z těchto příkazů:

- Pro produkt Windows:

```
SET MQIPADDRV=MQIPADDR_IPV4|MQIPADDR_IPV6
```

- Pro systémy UNIX and Linux :

```
export MQIPADDRV=MQIPADDR_IPV4|MQIPADDR_IPV6
```

NÁZEV MQNAME

Parametr MQNAME určuje název lokálního serveru NetBIOS , který mohou procesy produktu WebSphere MQ používat.

Úplný popis a pravidla priority na klientovi a na serveru viz “Definování připojení NetBIOS v systému Windows” na stránce 85 .

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 WebSphere MQ současně na klientovi WebSphere MQ MQI.

SERVER MQSERVER

Proměnná prostředí MQSERVER se používá k definování minimálního kanálu. Hodnota MQSERVER určuje umístění serveru WebSphere MQ a způsob komunikace, který má být použit.

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:

- Pro systémy Windows:

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

- Pro systémy UNIX and Linux :

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

TransportType může mít jednu z následujících hodnot, v závislosti na platformě klienta IBM WebSphere 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 konfigurujete správce front s více instancemi, můžete použít seznam *ConnectionName* k určení různých instancí správce front.

Předvolený port TCP/IP

Při výchozím nastavení pro TCP/IP produkt WebSphere 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 produkt Windows:

    ```
    SET MQSERVER=ChannelName/TransportType/ConnectionName(PortNumber)
    ```

  - Pro systémy UNIX and Linux :

    ```
    export MQSERVER='ChannelName/TransportType/ConnectionName(PortNumber)'
    ```

- Změna souboru `mqclient.ini` přidáním čísla portu na název protokolu, například:

  ```
  TCP:
  port=2001
  ```

- Přidání produktu WebSphere MQ do souboru služeb, jak je popsáno v tématu "Použití modulu listener protokolu TCP/IP" na stránce 92.

Výchozí soket SPX

Při výchozím nastavení produkt SPX WebSphere MQ předpokládá, 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)`. Jsou-li klient a server WebSphere MQ ve stejné síti, není třeba zadávat síť. 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 klienta WebSphere MQ MQI a serverovou počítačem, 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 systémuUNIX and 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:

- V systému Windows:

```
SET MQSERVER=
```

- Na systémech UNIX and 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 UNIX and Linux :

```
export MQSSLCRYP=string
```

Související odkazy

Parametr **ALTER QMGR** příkazu **SSLCRYP**

MQSSLFIPS

Funkce MQSSLFIPS určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, pokud je šifrování prováděno v produktu WebSphere 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 UNIX and Linux :

```
export MQSSLFIPS=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 UNIX and Linux :

```
export MQSSLKEYR=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 UNIX and 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.

Na systémech UNIX and Linux můžete například 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 UNIX and Linux :

```
export MQSSLRESET=integer
```

Řízení publikování/odběru ve frontě

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 .

Tabulka 23. Konfigurační parametry publikování a odběru

Popis	**Název parametru MQSC**
Počet opakování zprávy příkazu	**PSRTYCNT**
Zahodit nedoručitelnou vstupní zprávu příkazu	**PSNPMSG**
Chování po nedoručitelné zprávě s odpovědí příkazu	**PSNPRES**
Zprávy příkazů zpracování v synchronizačním bodě	**PSSYNCPT**

Sekce 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 zopakují.

  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 programu WebSphere MQ Explorer, 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

Poznámka: Pokud jste provedli migraci z produktu Version 6.0 , musíte produkt **strmqbrk** použít k migraci stavu zprostředkovatele publikování/odběru produktu Version 6.0 , pokud pracujete s upgradovaným správcem front. Tento parametr se nevztahuje na z/OS.

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

Rozhraní WebSphere MQ Explorer nebo příkaz **runmqsc** použijte k povolení rozhraní publikování/odběru ve frontě, pokud již rozhraní není povoleno.

Příklad

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

Jak pokračovat dále

Produkt WebSphere MQ zpracovává příkazy publikování/odběru ve frontě a volání rozhraní MQI (Message Queue Queue) rozhraní JMS (Message Queue Queue).

Zastavení publikování/odběru ve frontě

Než začnete

Publikování/odběr ve frontě je zamítnutý.

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 produkt WebSphere MQ Explorer nebo příkaz **runmqsc** .

Příklad

```
ALTER QMGR PSMODE(COMPAT)
```

Přidání proudu

Proudy můžete přidat ručně, aby koexistovaly s proudy migrovanými ze správců front Version 6.0 .

Než začnete

Přečtěte si téma Proudy a témataa seznamte se s tím, jak fungují proudy publikování/odběru.

Informace o této úloze

K provedení těchto kroků použijte příkaz PCF, **runmqsc**nebo IBM WebSphere MQ Explorer .

Poznámka: Kroky 1 a 2 můžete provádět v libovolném pořadí. Proveďte pouze krok 3 po dokončení kroků 1 a 2.

Postup

1. Definujte lokální frontu se stejným názvem jako proud Version 6.0 .
2. Definujte lokální téma se stejným názvem jako proud Version 6.0 .
3. Přidejte název fronty do seznamu názvů SYSTEM.QPUBSUB.QUEUE.NAMELIST .
4. Opakujte pro všechny správce front v produktu Version 7.1 nebo vyšší, kteří jsou v hierarchii publikování/odběru.

přidání 'Sport'

V příkladu sdílení proudu 'Sport' pracují správci front Version 6.0 a Version 7.1 ve stejné hierarchii publikování/odběru. Správci front produktu Version 6.0 sdílejí proud s názvem 'Sport'. Příklad ukazuje,

jak vytvořit frontu a téma pro Version 7.1 správce front s názvem 'Sport's řetězcem tématu 'Sport' , který je sdílen s proudem verze 6 'Sport'.

Version 7.1 Aplikace publikování, publikování do tématu 'Sport's řetězcem tématu 'Soccer/Results' vytvoří výsledný řetězec tématu 'Sport/Soccer/Results' . Ve správcích front systému Version 7.1 obdrží publikování odběratelé tématu 'Sport's řetězcem tématu 'Soccer/Results' .

Ve správcích front systému Version 6.0 obdrží publikování odběratelé proudu 'Sport' s řetězcem tématu 'Soccer/Results' .

```
runmqsc QM1
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM1.
define qlocal('Sport')
     1 : define qlocal('Sport')
AMQ8006: WebSphere MQ queue created.
define topic('Sport') topicstr('Sport')
     2 : define topic('Sport') topicstr('Sport')
AMQ8690: WebSphere 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: WebSphere MQ namelist changed.
```

Poznámka: Do příkazu **alter namelist** musíte zadat jak existující názvy v objektu seznamu názvů, tak i nové názvy, které přidáváte.

Jak pokračovat dále

Informace o proudu jsou předány ostatním zprostředkovatelům v hierarchii.

Pokud je zprostředkovatelem zprostředkovatel Version 6.0, spravujte jej jako zprostředkovatele Version 6.0 . To znamená, že máte možnost vytvořit frontu proudu ručně nebo nechat zprostředkovatele vytvořit frontu proudu dynamicky v případě potřeby. Fronta je založena na definici modelové fronty SYSTEM.BROKER.MODEL.STREAM.

Je-li zprostředkovatelem Version 7.1, musíte nakonfigurovat každého správce front Version 7.1 v hierarchii ručně.

Odstranění proudu

Proud můžete odstranit z produktu IBM WebSphere MQ Version 7.1nebo novější ve správci front.

Než začnete

Použití publikování/odběru ve frontě je zamítnuto v produktu IBM WebSphere MQ Version 7.1.

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.

Informace o této úloze

Pokyny k odstranění proudu z jakýchkoli správců front produktu Version 6.0 , ke kterým je připojen, najdete v tématu Odstranění proudu (ps11870_.htm v dokumentaci v6.0).

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

1. Zopakujte kroky 3 až 5 ve všech ostatních propojeném produktu Version 7.1nebo novějším správci front, který je hostitelem proudu.
2. Odeberte proud ze všech ostatních připojených serverů Version 6.0nebo starších správců front.

Přidání bodu odběru

Jak přidat bod odběru, který nebyl migrován z zprostředkovatele událostí produktu IBM WebSphere MQ nebo produktu IBM WebSphere MQ Message Broker produktem **migmbbrk**. Rozšířit existující aplikaci publikování/odběru ve frontě, kterou jste migrovali z produktu IBM WebSphere MQ Event Broker nebo IBM WebSphere MQ Message Broker s novým bodem odběru.

Než začnete

1. Dokončete migraci z produktu IBM WebSphere MQ Event Broker a IBM WebSphere MQ Message Broker Version 6.0 na IBM WebSphere MQ Version 7.1.
2. Ověřte, že bod odběru není v produktu SYSTEM.QPUBSUB.SUBPOINT.NAMELISTjiž definován.
3. Zkontrolujte, zda existuje objekt tématu nebo řetězec tématu se stejným názvem jako bod odběru.

Informace o této úloze

Existující aplikace zprostředkovatele událostí produktu IBM WebSphere MQ používají body odběru. Nové aplikace produktu IBM WebSphere MQ Version 7.1 nepoužívají body odběru, ale mohou spolupracovat s existujícími aplikacemi, které používají mechanizmus migrace bodu odběru.

Je možné, že bod odběru nebyl migrován **migmbbrk**, pokud v době migrace nebyl použit bod odběru.

Možná budete chtít přidat bod odběru do existujících programů publikování/odběru ve frontě převedených migrací z produktu IBM WebSphere MQ Event Broker.

Body odběru nepracují s programy publikování/odběru ve frontě, které používají záhlaví produktu MQRFH1 , která byla migrována z produktu IBM WebSphere MQ Version 6.0, nebo dříve.

Není třeba přidávat body odběru, které by používaly integrované aplikace pro publikování/odběr, které jsou napsány pro produkt IBM WebSphere MQ Version 7.1.

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 přidaných 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.

Připojení správce front k hierarchii zprostředkovatele

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

Než začnete

1. Povolit režim publikování/odběru ve frontě. Viz Spuštění publikování/odběru ve frontě.
2. Tato změna je šířena do nadřízeného správce front pomocí připojení IBM WebSphere MQ . Existují dva způsoby, jak navázat spojení.
   - Připojte správce front ke klastru IBM WebSphere MQ . Viz téma Přidání správce front do klastru .
   - Vytvořte připojení kanálu dvoubodového spojení s použitím přenosové fronty nebo aliasu správce front se stejným názvem jako nadřízený správce front. Další informace o způsobu vytvoření dvoubodového připojení kanálu naleznete v tématu WebSphere MQ techniky distribuovaného systému zpráv.

Informace o této úloze

Pomocí příkazu ALTER QMGR PARENT *(PARENT_NAME)* runmqsc připojte podřízené prvky k rodičům.

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

Postup

ALTER QMGR PARENT (PARENT)

Příklad

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

```
C:>runmqsc QM2
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM2
alter qmgr parent(QM1)
     1 : alter qmgr parent(QM1)
```

```
AMQ8005: WebSphere MQ queue manager changed.
display pubsub all
     2 : display pubsub all
AMQ8723: Display pub/sub status details.
   QMNAME(QM2)                             TYPE(LOCAL)
   STATUS(ACTIVE)
AMQ8723: Display pub/sub status details.
   QMNAME(QM1)                             TYPE(PARENT)
   STATUS(ACTIVE)
```

Následující příklad zobrazuje výsledek dotazování QM1 na jeho připojení:

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

Jak pokračovat dále

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

Související pojmy

Proudy a témata

Úvod do systému zpráv publikování/odběru produktu WebSphere MQ

Související odkazy

ZOBRAZIT PUBSUB

Odpojení správce front od hierarchie zprostředkovatele

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

Informace o této úloze

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

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

Postup

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

Příklad

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

Jak pokračovat dále

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

Konfigurace klastru správce front

Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

Než začnete

Úvod do problematiky klastrování najdete v následujících tématech:

- Jak fungují klastry
- “Porovnání klastrování a distribuovaných front” na stránce 158
- “Komponenty klastru” na stránce 160

Když navrhujete klastr správců front, musíte provést některá rozhodnutí. Nejprve se musíte rozhodnout, kteří správci front v klastru mají uchovávat úplná úložiště informací o klastru. Jakýkoli správce front, kterého vytvoříte, může pracovat v klastru. Pro tento účel si můžete vybrat libovolný počet správců front, ale ideální počet je dva. Informace o výběru správců front za účelem zadržení úplných úložišť naleznete v tématu “Jak vybrat správce front klastru k uchování úplných úložišť” na stránce 173.

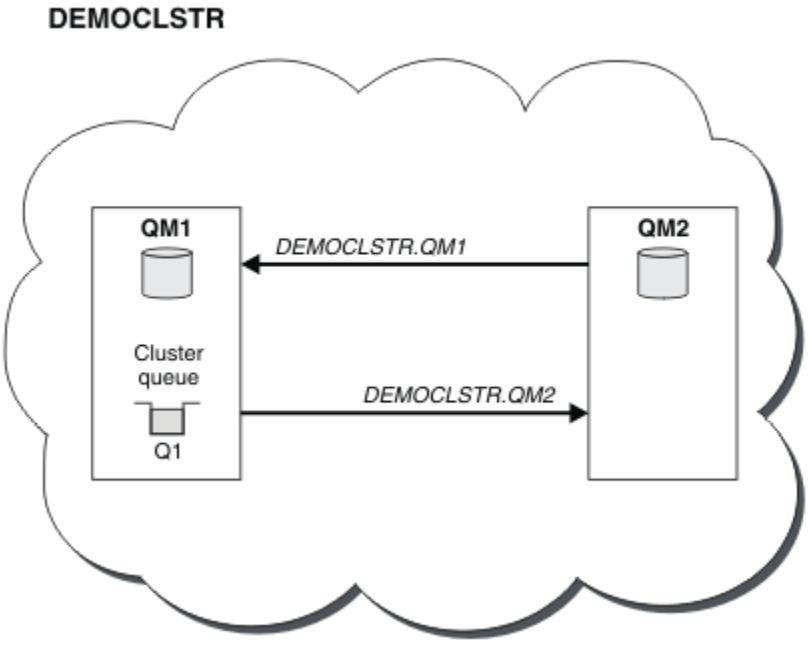
Další informace o návrhu klastru naleznete v následujících tématech:

- “Uspořádání klastru” na stránce 175
- “Konvence pojmenování klastrů” na stránce 175
- “Překrývání klastrů” na stránce 176

Příklad

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

Obrázek 21 na stránce 156 znázorňuje klastr s názvem DEMOCLSTR se dvěma správci front nazvaným QM1 a QM2.



Obrázek 21. Malý klastr dvou správců front

- Správci front mají dlouhé názvy, jako například LONDON a NEWYORK. Stejné názvy se používají v rozšířených úlohách a v úlohách vyrovnávání pracovní zátěže. V produktu IBM WebSphere MQ for z/OSjsou názvy správců front omezeny na čtyři znaky.
- Názvy správců front implikují, že každý správce front je na samostatném počítači. Tyto úlohy byste mohli provádět se všemi správci front na stejném počítači.
- Úlohy používají skriptové příkazy produktu IBM WebSphere MQ , jak by jej zadal administrátor systému pomocí příkazů **MQSC** . Existují i jiné způsoby zadávání příkazů, včetně použití snadnějšího Průzkumníka IBM WebSphere MQ . Místo použití skriptových příkazů produktu WebSphere MQ je demonstrovat, které příkazy IBM WebSphere MQ se používají v úlohách.

Pokyny pro nastavení podobného vzorového klastru najdete v tématu “Nastavení nového klastru” na stránce 181.

Jak pokračovat dále

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

- “Ustanovení komunikace v klastru” na stránce 178
- “Správa klastrů produktu IBM WebSphere MQ” na stránce 181
- “Směrování zpráv do a z klastrů” na stránce 242
- “Použití klastrů pro správu pracovní zátěže” na stránce 255

Další informace, které vám pomohou při konfiguraci klastru, najdete v tématu “Rady pro klastrování” na stránce 177.

Související pojmy

Klastry

Řízení přístupu a více přenosových front klastru

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

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

Lokální kontroly se provádějí proti frontě, kterou aplikace otevírá. V distribuovaném řazení do fronty aplikace obvykle otevře definici vzdálené fronty a dojde k pokusu o přístup k definici vzdálené fronty. Je-li zpráva vložena s celým záhlavím směrování, jsou kontroly provedeny v přenosové frontě. Pokud aplikace otevře frontu klastru, která není na lokálním správci front, neexistuje lokální objekt, který by bylo možné zkontrolovat. Kontrola řízení přístupu se provádí proti přenosové frontě klastru, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Dokonce i v případě více přenosových front klastru z produktu Version 7.5jsou kontroly lokálního řízení přístupu pro vzdálené fronty klastru prováděny vůči produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE.

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

Od produktu Version 7.1mají administrátoři další způsob, jak nastavit řízení přístupu pro fronty klastru. Pomocí příkazu **setmqaut** můžete vytvořit profil zabezpečení pro frontu klastru na libovolném správci front v klastru. Tento profil se projeví, pokud otevřete vzdálenou frontu klastru lokálně a uvedete pouze

název fronty. Také můžete nastavit profil pro vzdáleného správce front. Pokud tak učiníte, může správce front zkontrolovat profil uživatele, který otevře frontu klastru, a to tak, že poskytne úplný název.

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

Tip: Změny prováděné ve frontě klastru při přístupu ke kontrole v produktu Version 7.1 se nevztahují na vzdálené fronty. Kontroly přístupu se stále provádějí proti místním definicím. Změny znamenají, že můžete postupovat podle stejného přístupu ke konfiguraci kontroly přístupu u front klastru a témat klastru.

Související pojmy

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

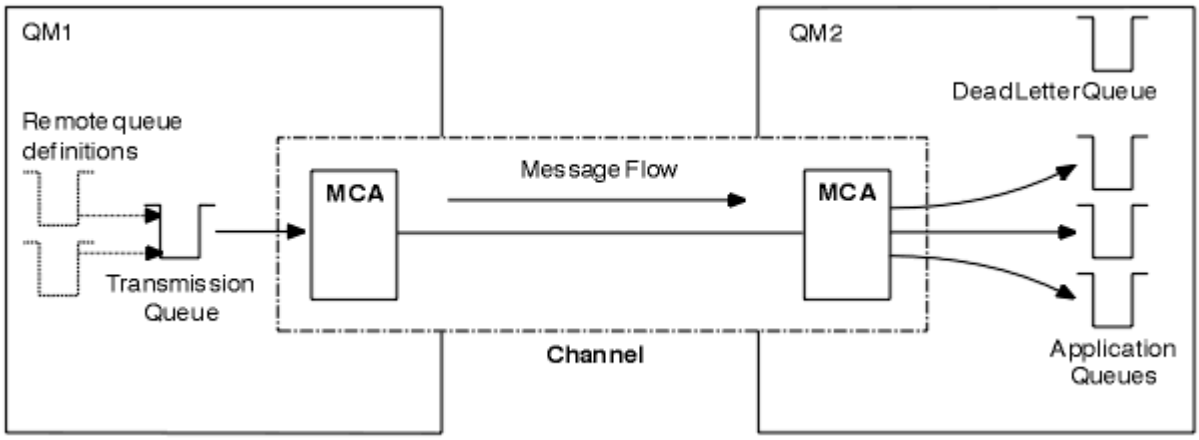
Porovnání klastrování a distribuovaných front

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

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

- Přenosová fronta
- Kanál pro vzdáleného správce front

Obrázek 22 na stránce 158 zobrazuje komponenty požadované pro distribuované řazení do fronty.



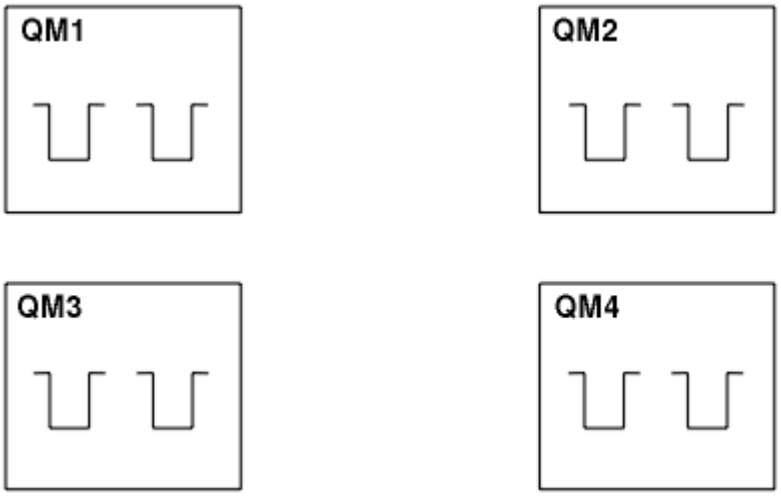
Obrázek 22. distribuované fronty

Pokud seskupíte správce front v klastru, budou fronty v libovolném správci front k dispozici všem ostatním správcům front v klastru. Kterýkoli správce front může odeslat zprávu libovolnému jinému správci front ve stejném klastru bez explicitních definic. Neposkytujete definice kanálu, definice vzdálených front nebo přenosové fronty pro každý cíl. Každý správce front v klastru má jednu přenosovou frontu, ze které může přenášet zprávy do libovolného jiného správce front v klastru. Každý správce front v klastru potřebuje definovat pouze:

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

Definice pro nastavení klastru oproti distribuovanému řazení do fronty

Podívejte se na Obrázek 23 na stránce 159, kde se zobrazují čtyři správci front s dvěma frontami. Uvažte, kolik definic je zapotřebí k připojení těchto správců front pomocí distribuovaných front. Porovnejte, kolik definic je třeba pro nastavení stejné sítě jako klastru.



Obrázek 23. Síť čtyř správců front

Definice pro nastavení sítě pomocí distribuovaných front

Chcete-li nastavit síť zobrazenou v produktu Obrázek 22 na stránce 158 pomocí distribuovaných front, můžete mít tyto definice:

Tabulka 24. Definice pro distribuované ukládání do fronty

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

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

Definice k nastavení sítě pomocí klastrů

Chcete-li nastavit síť zobrazenou v produktu Obrázek 22 na stránce 158 pomocí klastrů, musíte mít následující definice:

Tabulka 25. Definice pro klastrování		
Popis	**Počet na správce front**	**Celkový počet**
Definice odesílacího kanálu klastru pro kanál, v němž mají být odesílány zprávy do správce front úložiště	1	4
Definice přijímacího kanálu klastru pro kanál, na kterém mají být přijímány zprávy od jiných správců front v klastru	1	4
Definice lokální fronty pro každou lokální frontu	2	8

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

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

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

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

- Názvy objektů se vždy shodují, například jméno kanálu v páru odesilatel-příjemce.
- Název přenosové fronty zadaný v definici kanálu se vždy shoduje se správnou definicí přenosové fronty nebo názvem přenosové fronty, která je určena v definici vzdálené fronty.
- Definice QREMOTE vždy ukazuje na správnou frontu ve vzdáleném správci front.

Jakmile je klastr nastaven, můžete přesunout fronty klastru z jednoho správce front do jiného v rámci klastru, aniž byste museli provádět jakoukoli správu systému na kterémkoli jiném správci front. Není žádná možnost zapomenout na odstranění nebo upravit definice kanálu, vzdálené fronty nebo definice přenosové fronty. Do klastru můžete přidávat nové správce front bez jakéhokoli narušení existující sítě.

Komponenty klastru

Klastry se skládají z správců front, klastrovaných úložišť, kanálů klastru a front klastru.

Informace o jednotlivých komponentách klastru najdete v následujících dílčích tématech:

Související pojmy

Klastry

“Porovnání klastrování a distribuovaných front” na stránce 158
Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

“Správa klastrů produktu IBM WebSphere MQ” na stránce 181
Klastry IBM WebSphere MQ můžete vytvářet, rozšiřovat a udržovat.

Související úlohy

“Konfigurace klastru správce front” na stránce 156
Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

“Nastavení nového klastru” na stránce 181
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.

Úložiště klastru

Úložiště je kolekce informací o správcích front, kteří jsou členy klastru.

Informace o úložišti obsahují názvy správců front, jejich umístění, kanály, které hostují, a další informace. Informace se ukládají ve formě zpráv ve frontě s názvem SYSTEM.CLUSTER.REPOSITORY.QUEUE. Fronta je jedním z výchozích objektů. Je definován při vytváření správce front produktu WebSphere MQ , s výjimkou produktu WebSphere MQ for z/OS.

Dva správci front v klastru obvykle obsahují úplné úložiště. Zbývající správci front mají všechny zadržené dílčí úložiště.

Úplné úložiště a částečné úložiště

Správce front, který je hostitelem úplné sady informací o každém správci front v klastru, má úplné úložiště. Ostatní správci front v klastru mají dílčí úložiště obsahující dílčí sadu informací v úplných úložištích.

Částečné úložiště obsahuje informace o pouze těch správcích front, s nimiž správce front potřebuje vyměňovat zprávy. Správci front žádají o aktualizace informací, které potřebují, takže pokud se změní, správce front úplného úložiště jim odešle nové informace. Pro většinu času obsahuje dílčí úložiště všechny informace, které správce front potřebuje provést v rámci klastru. Pokud některý správce front potřebuje další informace, vyžádá si je z úplného úložiště a poté provede aktualizaci svého dílčího úložiště. Správci front používají frontu s názvem SYSTEM.CLUSTER.COMMAND.QUEUE k vyžádání a přijímání aktualizací do úložišť. Tato fronta je jedním z výchozích objektů.

Správce front klastru

Správce front klastru je správce front, který je členem klastru.

Jeden správce front může být členem více klastrů. Každý správce front klastru musí mít název, který je jedinečný v rámci všech klastrů, jejichž je členem.

Správce front klastru může být hostitelem front, které inzeruje k ostatním správcům front v klastru. Správce front klastru nemusí hostitele ani inzerovat žádné fronty. Může odesílat zprávy do klastru a přijímat pouze odpovědi, které jsou adresovány explicitně, a nikoli do inzerovaných front.

V produktu WebSphere MQ for z/OSmůže být správce front klastru členem skupiny sdílení front. V tomto případě sdílí své definice front s ostatními správci front ve stejné skupině sdílení front.

Správci front klastru jsou nezávislí. Mají plnou kontrolu nad frontami a kanály, které definují. Jejich definice nemohou být upraveny jinými správci front (jinými než správci front ve stejné skupině sdílení front). Správci front úložiště neřídí definice v jiných správcích front v klastru. Mají kompletní sadu všech definic, pro použití v případě potřeby. Klastr je federace správců front.

Po vytvoření nebo změně definice ve správci front klastru se tyto informace odešlou do správce front úplného úložiště. Ostatní úložiště v klastru jsou aktualizována později.

Správce front úplného úložiště

Správce front úplného úložiště je správce front klastru, který obsahuje úplnou reprezentaci prostředků klastru. Chcete-li zajistit dostupnost, nastavte dva nebo více správců front úplného úložiště v každém klastru. Správci front úplného úložiště obdrží informace odeslané ostatními správci front v klastru a aktualizují svá úložiště. Posílají si navzájem zprávy, aby si byli jisti, že jsou oba udržovány v aktuálním stavu s novými informacemi o klastru.

Správci front a úložiště

Každý klastr má alespoň jeden (nejlépe dva) správce front, v nichž jsou umístěna úplná úložiště informací o správcích front, frontách a kanálech v klastru. Tato úložiště také obsahují požadavky od ostatních správců front v klastru pro aktualizace informací.

Ostatní správci front, kteří obsahují dílčí úložiště, obsahují informace o podmnožině front a správců front, s nimiž potřebují komunikovat. Správci front vytvářejí svá dílčí úložiště tím, že provádějí dotazy v případě, že nejprve potřebují přistupovat k jiné frontě nebo správci front. Požadují, aby byly upozorněny na všechny nové informace týkající se této fronty nebo správce front.

Každý správce front ukládá své informace o úložišti ve zprávách ve frontě s názvem SYSTEM.CLUSTER.REPOSITORY.QUEUE. Správci front si vyměňují informace o úložišti ve zprávách ve frontě s názvem SYSTEM.CLUSTER.COMMAND.QUEUE.

Každý správce front, který spojuje klastr, definuje odesílatele klastru, CLUSSDR, kanál na jedno z úložišť. Okamžitě se dozví, které ostatní správci front v klastru mají úplná úložiště. Od té doby může správce front požadovat informace z některého z úložišť. Odešle-li správce front informace do vybraného úložiště, odešle také informace do jiného úložiště (je-li k dispozici).

Úplné úložiště je aktualizováno, když správce front, který je hostitelem, obdrží nové informace od jednoho z správců front, který je k němu připojen. Nové informace jsou také odeslány do jiného úložiště, aby se snížilo riziko zpoždění v případě, že správce front úložiště není ve službě. Jelikož jsou všechny informace odeslány dvakrát, úložiště musí zahodit duplikáty. Každá položka informací nese pořadové číslo, které úložiště používají k identifikaci duplikátů. Všechna úložiště jsou postupně mezi sebou ve výměně zpráv.

Fronty 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, jehož hostitelem je fronta. 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 směrování a vloží zprávu do přenosové fronty klastru.

Fronta klastru může být fronta, kterou sdílí členové skupiny sdílení front v produktu IBM WebSphere 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

S výjimkou produktu z/OSmůže správce front ukládat zprávy pro ostatní správce front v 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 vyhrazené SYSTEM.CLUSTER.TRANSMIT.QUEUES se správcem front, který byl upgradován z dřívější verze produktu, ujistěte se, že SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE má volbu SHARE/NOSHARE nastavenou na **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 správcích 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 se standardně vytvoří ve všech správe správců front s výjimkou produktu z/OS.

Na jiných platformách než z/OSmůžete nakonfigurovat správce front tak, aby přenášecí zprávy do jiných klastrovaných správců front používal 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 rozděleným 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 WebSphere MQ automaticky vytvoří definici ekvivalentní definici vzdálené fronty, aby bylo možné zprávu odeslat.

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 odkazy

Název ClusterChannel(MQCHAR20)

Kanály klastru

Pro správce front v klastru musíte definovat příjemce klastru a odesílací kanály klastru. Speciální pokyny platí pro úplná úložiště.

V rámci klastrů jsou zprávy rozděleny mezi správci front klastru na speciální typ kanálu, pro který potřebujete definice kanálu příjemce klastru a definice odesílacího kanálu klastru.

Kanál odesílatele klastru: CLUSSDR

Ručně definujte odesílací kanál klastru k úplnému úložišti na každém správci front v klastru. Definice odesílatele klastru umožňuje správci front navázat počáteční kontakt s klastrem. Určuje název správce front úplného úložiště, do kterého správce front preferuje odeslání informací o klastru. Odesílací kanál klastru se používá k upozornění na úložiště všech změn stavu správce front. Například, pokud je fronta přidána nebo odebrána. Je používán také k přenosu zpráv.

Samotní správci front mají odesílací kanály klastru, které jsou nasměrovány na sebe navzájem. Používají je ke vzájemné výměně změn stavu klastru.

Je velmi důležité, aby úplné úložiště ukazovala na definici kanálu CLUSSDR . Po provedení úvodního kontaktu jsou další objekty správce front klastru definovány automaticky podle potřeby. Správce front může odesílat informace o klastru do všech úplných úložišť a zpráv do každého správce front.

Definice CLUSSDR provedené v úplných správcích front úložiště jsou speciální. Všechny aktualizace vyměňované v úplných úložištích jsou přenášeny výhradně na tyto kanály. Administrátor explicitně řídí síť úplných úložišť. Administrátor musí definovat kanál CLUSSDR z každého správce front úplného úložiště do všech ostatních správců front úplného úložiště v klastru. Administrátor musí ručně vytvořit definice CLCLSDR na správci front úplného úložiště a nenechávat je automaticky definovat.

Odesílací kanály klastru musí být definovány pouze pro připojení dílčího úložiště k úplnému úložišti nebo pro připojení dvou úplných úložišť dohromady. Ruční konfigurace kanálu CLUSSDR , který adresuje dílčí úložiště, nebo správce front, který není v klastru, vede k chybovým zprávám, například AMQ9427 a AMQ9428 , které se vydávají.

Ačkoli to může být někdy nevyhnutelné jako dočasná situace (například když upravujete umístění úplného úložiště), měly by být nesprávné definice odstraněny co nejdříve, aby se tyto chyby mohly zastavit.

Přijímací kanál klastru: CLUSRCVR

Definice přijímacího kanálu klastru definuje konec kanálu, v němž může správce front klastru přijímat zprávy od jiných správců front v klastru.

Přijímací kanál klastru může také přenášet informace o klastru-informace určené pro lokální úložiště. Definováním kanálu příjemce klastru zobrazuje správce front ostatní správce front klastru, kterého je k dispozici pro příjem zpráv. Pro každého správce front klastru je nutný alespoň jeden přijímací kanál klastru.

Definice CLUSRCVR umožňuje jiným správcům front automaticky definovat odpovídající definice kanálu CLUSSDR .

Související pojmy

“Automatická definice kanálů klastru” na stránce 165
Před odesláním zprávy do vzdáleného místa určení musí mít správce front definici pro odesílací kanál klastru. Po uvedení správce front do klastru provedením počátečních definic CLUSSDR a CLUSRCVR produkt WebSphere MQ automaticky vytvoří definice kanálu odesílatele klastru, když je třeba. Automaticky definované kanály odesílatele klastru nelze upravovat. Jejich chování lze upravit pomocí uživatelské procedury automatické definice kanálu.

Automatická definice kanálů klastru

Před odesláním zprávy do vzdáleného místa určení musí mít správce front definici pro odesílací kanál klastru. Po uvedení správce front do klastru provedením počátečních definic CLUSSDR a CLUSRCVR produkt WebSphere MQ automaticky vytvoří definice kanálu odesílatele klastru, když je třeba. Automaticky definované kanály odesílatele klastru nelze upravovat. Jejich chování lze upravit pomocí uživatelské procedury automatické definice kanálu.

Je-li definován koncový bod odesílatele klastru i konec kanálu příjemce klastru, bude kanál spuštěn. Automaticky definovaný kanál zůstane aktivní, dokud není nadále potřebný a je vypnut pomocí normálních pravidel pro odpojení.

Automaticky definované kanály odesílatele klastru získávají své atributy z příslušné definice přijímacího kanálu klastru v přijímajícím správci front. I když existuje ručně definovaný odesílací kanál klastru, jeho atributy se automaticky upraví, aby se zajistilo, že se shodují s odpovídající definicí příjemce klastru. Předpokládejme například, že jste definovali parametr CLUSRCVR bez uvedení čísla portu v parametru CONNAME , a ručně definujte CLUSSDR , která určuje číslo portu. Když automaticky definovaná hodnota CLUSSDR nahradí ručně definovanou hodnotu, bude číslo portu (převzato z CLUSRCVR) prázdné. Použije se výchozí číslo portu a kanál selže.

V automaticky definované definici odesílatele klastru nelze upravit definici.

Pomocí příkazu DISPLAY CHANNEL **runmqsc** nelze zobrazit automaticky definované kanály. Chcete-li zobrazit automaticky definované kanály, použijte příkaz:

```
DISPLAY CLUSQMGR(qMgrName)
```

Chcete-li zobrazit stav automaticky definovaného kanálu CLUSSDR odpovídající definici kanálu CLUSRCVR , kterou jste vytvořili, použijte následující příkaz:

```
DISPLAY CHSTATUS(channelname)
```

Uživatelská procedura automatické definice kanálu produktu WebSphere MQ můžete použít k zápisu uživatelského ukončovacího programu pro přizpůsobení kanálu odesílatele klastru nebo kanálu příjemce klastru. V prostředí klastru můžete použít uživatelskou proceduru s automatickou definicí kanálu s následujícími prvky:

- Definice komunikačních prostředků, které jsou, tj. SNA LU6.2
- Přidat nebo odebrat jiné uživatelské procedury, například uživatelské procedury pro zabezpečení zprávy
- Změňte názvy uživatelských procedur kanálu. Je třeba změnit název uživatelské procedury kanálu CLUSSDR , protože název uživatelské procedury kanálu CLUSSDR je automaticky generován z definice kanálu CLUSRCVR . Automaticky generovaný název může být chybný a téměř jistě je chybný, pokud se dva konce kanálu nacházejí na různých platformách. Formát názvů uživatelských procedur se liší na různých platformách. Například v systému Windows je, SCYEXIT('*drive*:*path**library*(secexit)').

Názvy uživatelských procedur na jiných platformách než z/OS mají obecný tvar *cesta*/*knihovna*(*funkce*). Je-li přítomen *funkce* , použije se až osm znaků. Jinak se použije *knihovna*, zkrácená na osm znaků. Například

- `/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`

Chcete-li povolit odchozí kanál (TCP) pro použití konkrétní adresy IP, portu nebo rozsahu portů, použijte atribut kanálu `LOCLADDR`. Parametr `LOCLADDR` je užitečný v případě, že máte 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, musíte napsat uživatelskou proceduru automatické definice kanálu, abyste vynutili hodnotu `LOCLADDR` do libovolného ze svých automaticky definovaných kanálů `CLUSSDR` , a vy jej musíte zadat v ručně definovaném kanálu `CLUSSDR` .

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` .

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.

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.

Automaticky definované definice odesílacího kanálu klastru nejsou skutečnými objekty kanálu. Na jiných platformách než z/OSsi produkt OAM (správce oprávnění k objektu) neví o své existenci. Pokusíte-li se zadat příkazy start, stop, ping, reset nebo resolve na automaticky definovaných odesílacích kanálech klastru, OAM zkontroluje, zda máte oprávnění provést stejnou akci na přijímacím kanálu klastru pro klastr.

Pokud musí klastr použít funkci PROPCTL k odebrání záhlaví aplikací, například RFH2 , ze zpráv, které pochází ze správce front produktu WebSphere MQ verze 7, do správce front na dřívější úrovni produktu WebSphere MQ, je třeba, aby byla uživatelská procedura pro automatické definování kanálu zapsána, která vynutí funkci PROPCTL na hodnotu NONE. Ukončení je nutné, protože kanály odesílatele klastru mají svou definici založenou na odpovídajících přijímacích kanálech klastru. Vzhledem k tomu, že kanál příjemce klastru s dřívější úrovní nemá atribut PROPCTL, je atribut nastaven na hodnotu COMPAT pomocí kanálu odesílatele automatického klastru. Atribut je nastaven na COMPAT bez ohledu na to, co je nastaveno na manuálním kanálu odesílatele klastru.

Související odkazy

Lokální adresa (LOCLADDR)

Výchozí objekty klastru

Při použití klastrů WebSphere MQ vytvořte výchozí objekty klastru. Jsou zahrnuty do sady výchozích objektů automaticky vytvořených při definování správce front.

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`.

`SYSTEM.CLUSTER.COMMAND.QUEUE`

Každý správce front v klastru má lokální frontu s názvem `SYSTEM.CLUSTER.COMMAND.QUEUE` , která se používá k přenosu zpráv do úplného úložiště. Zpráva obsahuje všechny nové nebo změněné informace o správci front nebo o požadavcích na informace o ostatních správcích front. `SYSTEM.CLUSTER.COMMAND.QUEUE` je normálně prázdný.

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.REPOSITORY.QUEUE
Každý správce front v klastru má lokální frontu s názvem SYSTEM.CLUSTER.REPOSITORY.QUEUE. Tato fronta se používá k ukládání všech úplných informací o úložišti. Tato fronta není obvykle prázdná.

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. Produkt SYSTEM.CLUSTER.TRANSMIT.QUEUEnelze 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*.

SYSTEM.DEF.CLUSRCVR
Každý klastr má výchozí definici kanálu CLUSRCVR s názvem SYSTEM.DEF.CLUSRCVR. SYSTEM.DEF.CLUSRCVR se používá k zadání výchozích hodnot pro všechny atributy, které neurčujete při vytváření přijímacího kanálu klastru na správci front v klastru.

SYSTEM.DEF.CLUSSDR
Každý klastr má výchozí definici kanálu CLUSSDR s názvem SYSTEM.DEF.CLUSSDR. SYSTEM.DEF.CLUSSDR se používá k zadání výchozích hodnot pro všechny atributy, které při vytváření kanálu odesílatele klastru ve správci front v klastru nezadáte.

Přenosové fronty klastru a odesílací kanály klastru

Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru.

Zobrazíte-li odesílací kanál klastru, uvidíte, že je přidružen k přenosové frontě. 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. 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 168 popisuje proces výběru výchozí přenosové fronty; “Výběr ručně definovaných přenosových front pomocí kanálů odesílatele klastru” na stránce 169 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 170 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 změníte 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 doby, než budou klastrovaná spojení Version 7.5 sdílena s jednoduchou přenosovou frontou klastru, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Počínaje produktem Version 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. Další informace jsou uvedeny v tématech “Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278 a “Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 201.

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 mechanizmem přenosové fronty klastru nebo ruční konfigurací.

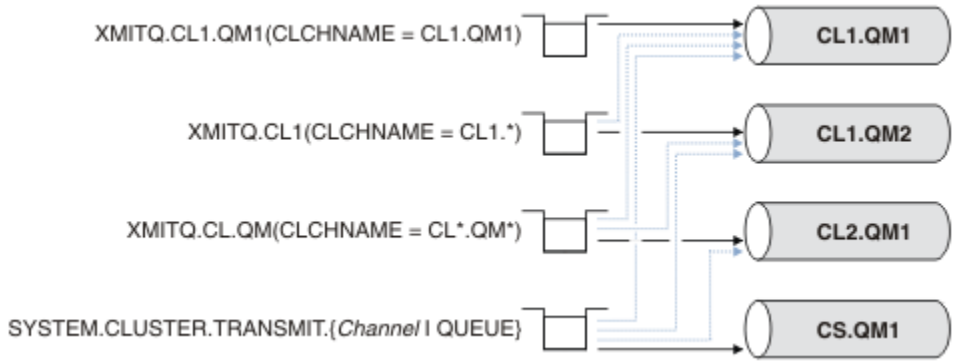
Výchozí přenosová fronta klastru je nastavena jako atribut správce front, **DEFCLXQ**. Jeho hodnota je buď SCTQ , nebo CHANNEL. Noví a migrovaní správci front jsou nastavovali na hodnotu SCTQ. Tuto hodnotu můžete změnit na CHANNEL.

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 otevírají 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 tématu Obrázek 24 na stránce 169. 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 24. 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 24 na stránce 169 zobrazuje přidružení mezi přenosovou frontou a odesílacími kanály klastru. Černé šipky ukazují skutečné svazy a šedé šípy, potenciální svazy. Pořadí priorit přenosových front v produktu Obrázek 24 na stránce 169 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, vyhnete 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 mezerovém 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 přerušen, 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. Přechodný proces přepnutí přenese 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 chyb 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.QUEUEa nikoli pro profily pro konkrétní přenosovou frontu klastru. Chcete-li aplikovat podrobnější kontroly zabezpečení, prohlédněte si téma “Řízení přístupu a více přenosových front klastru” na stránce 157.

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. Kde je volba odesílacích kanálů 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.

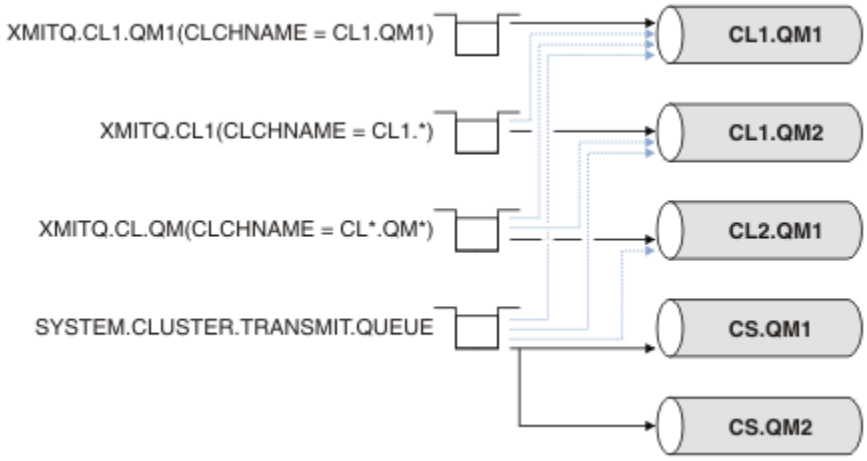
V systémech Obrázek 25 na stránce 172, CL1.QM1, CL1.QM2 a CS.QM1 jsou všechny kanály, které mohou vést ke stejnému cíli. Pokud například definujete Q1 v CL1 na QM1 a QM2 pak CL1.QM1 a CL1.QM2 obě poskytují přenosové cesty ke stejnému cíli, Q1, na dvou různých správcích front. Je-li kanál CS.QM1 také 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 máte v úmyslu 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 potom 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 přenese zprávu do jiné přenosové fronty.

V produktu Obrázek 25 na stránce 172jsou k výchozí přenosové frontě systému přidruženy dva kanály odesílatele klustru `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 25. 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 přenese 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 změnami restartů, spustí proces přepínání přenosové fronty, viz “Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje” na stránce 170.

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

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275

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

“Výpočet velikosti protokolu” na stránce 391
Odhadování velikosti protokolu, které správce front potřebuje.

Související úlohy

“Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

“Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 193
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 198
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 201
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.

Jak vybrat správce front klastru k uchování úplných úložišť

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

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

Obrázek 26. Dvě připojená úplná úložiště.

Každý další správce front v klastru udržuje obrázek o tom, co aktuálně ví o stavu klastru v *částečném úložišti*. Tito správci front publikují informace o sobě a žádají o informace o ostatních správcích front za použití jakýchkoli dvou dostupných úplných úložišť. Není-li vybrané úplné úložiště k dispozici, použije se další. Jakmile bude zvolené úplné úložiště opět dostupné, shromáždí nejnovější nové a změněné informace od ostatních, aby bylo možné pokračovat v kroku. Pokud všechna úplná úložiště nepůjdou mimo provoz, ostatní správci front použijí informace, které mají ve svých dílčích úložištích. Jsou však

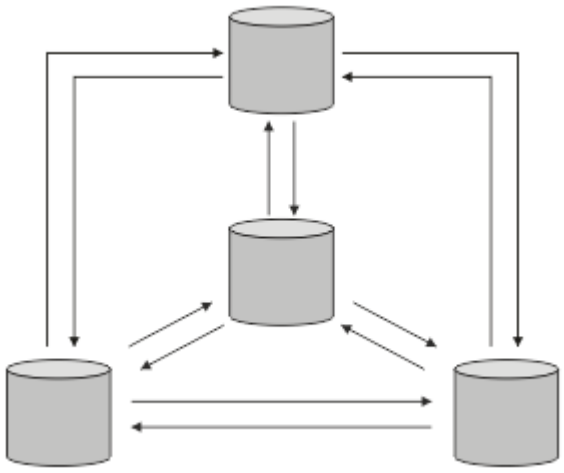
omezeny na používání informací, které mají; nové informace a požadavky na aktualizace nelze zpracovat. Když se úplná úložiště znovu připojí k síti, dochází k výměně zpráv za účelem uvedení všech úložišť (úplné i částečné) až do data.

Při plánování přidělení úplných úložišť uveďte následující aspekty:

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

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

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



Obrázek 27. Více než dvě připojená úplná úložiště

Související informace

MQ Clustery: Proč pouze dvě Úplná úložiště?
Jak velký může být klastr MQ ?

Uspořádání klastru

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

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

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

Konvence pojmenování klastrů

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

Doporučené postupy při pojmenování klastrů produktu MQ

Ačkoli názvy klastrů mohou mít až 48 znaků, při použití konvencí pojmenování na jiné objekty jsou užitečné poměrně krátké názvy klastrů. Viz “Doporučené postupy při výběru názvů kanálů klastru” na stránce 175.

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

Doporučené postupy při výběru názvů správců front klastru

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

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

Doporučené postupy při výběru názvů kanálů klastru

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

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

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

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

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

- CLUSTER1.QM1.T4

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

Pojmenování definic sdílených kanálů

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

Starší konvence pojmenování kanálů

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

Překrývání klastrů

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

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

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

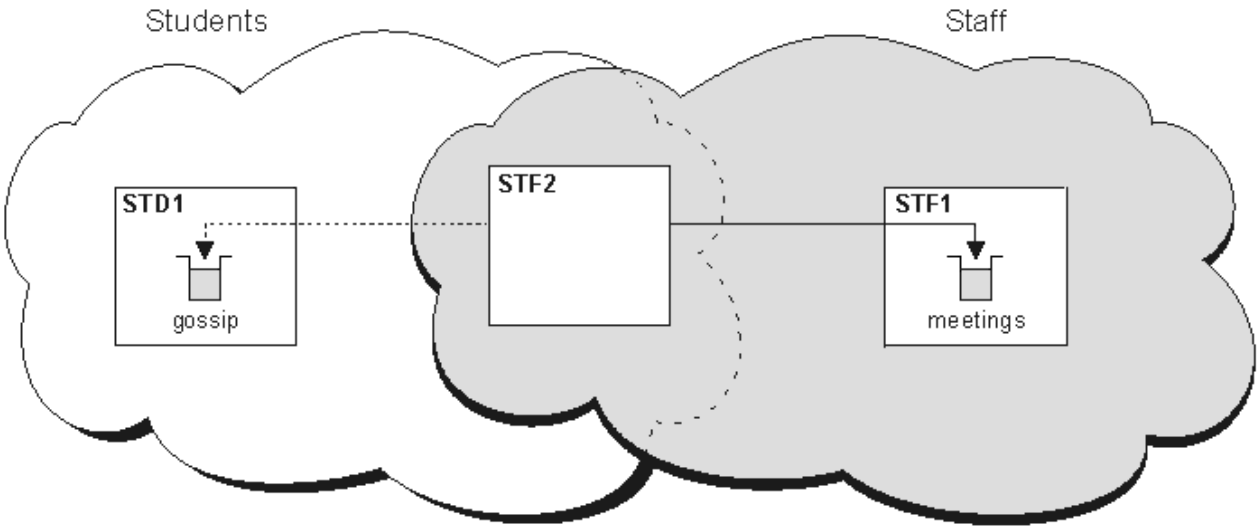
V produktu Obrázek 28 na stránce 177je správce front STF2 členem obou klastrů. Je-li správce front členem více než jednoho klastru, můžete využít výhody seznamů názvů a snížit počet definic, které potřebujete. Seznamy názvů obsahují seznam názvů, například názvy klastrů. Můžete vytvořit pojmenování seznamu názvů klastrů. Specify the namelist on the ALTER QMGR command for STF2 to make it a full repository queue manager for both clusters.

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

Definování tříd služeb

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

Chcete-li jasně rozlišovat mezi zaměstnanci a studenty, mohli byste jejich správce front seskupit do dvou klastrů, jak ukazuje Obrázek 28 na stránce 177. Produkt WebSphere MQ přesouvá zprávy do fronty schůzek v klastru personálu pouze prostřednictvím kanálů, které jsou definovány v daném klastru. Zprávy pro frontu pomluvy v klastru studentů přejdou přes kanály definované v daném klastru a přijmou odpovídající provozní třídu.



Obrázek 28. Třídy služeb

Rady pro klastrování

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

- Průzkumník WebSphere MQ nemůže přímo spravovat správce front WebSphere MQ pro správce front produktu z/OS verze starší než verze 6.0.
- Chcete-li přistupovat k frontám klastru, je třeba přidat definice ručních konfigurací do správců front mimo klastr.
- Pokud sloučíte dva klastry se stejným názvem, nemůžete je oddělit znovu. Proto je vhodné poskytnout všem klastrům jedinečný název.
- Pokud zpráva dorazí do správce front, ale neexistuje žádná fronta, kterou by bylo možné přijmout, zpráva se umístí do fronty nedoručených zpráv. Pokud fronta nedoručených zpráv neexistuje, kanál se znovu nezdaří a pokusí se o něj znovu. Použití fronty nedoručených zpráv je stejné jako u distribuovaných front.
- Integrita trvalých zpráv se udržuje. Zprávy nejsou duplikovány ani ztraceny jako výsledek použití klastrů.
- Použití klastrů snižuje administraci systému. Klastry usnadňují připojení větších sítí k mnoha dalším správcům front, než byste byli schopni uvažovat o použití distribuovaných front. Pokud se pokusíte povolit komunikaci mezi každým správcem front v klastru, hrozí nebezpečí, že budete spotřebovávat nadměrné síťové prostředky.
- Používáte-li průzkumníka WebSphere MQ Explorer, který prezentuje správce front ve stromové struktuře, může být zobrazení velkých klastrů příliš náročné.
- Produkt WebSphere MQ Explorer může spravovat klastr s správci front úložiště v produktu WebSphere MQ for z/OS verze 6 nebo novější. Není třeba jmenovat další úložiště na odděleném systému. U starších verzí produktu WebSphere MQ v systému z/OSprodukt WebSphere MQ Explorer nemůže spravovat klastr se správci front úložiště. Je třeba určit další úložiště v systému, který může produkt WebSphere MQ Explorer spravovat.
- Účelem distribučních seznamů je použít jediný příkaz MQPUT k odeslání stejné zprávy do více míst určení. Distribuční seznamy jsou podporovány v produktu WebSphere MQ pro systémy AIX, IBM i, HP-UX, Solaris, Linuxa Windows. Můžete použít distribuční seznamy s klastry správců front. V klastru jsou všechny zprávy rozbaleny v čase MQPUT . Výhoda, co se týče síťového provozu, není tak velká jako v neklastrovém prostředí. Výhoda distribučních seznamů je taková, že četné kanály a přenosové fronty nemusí být definovány manuálně.
- Budete-li používat klastry pro vyvážení zátěže, prozkoumejte své aplikace. Zjistěte, zda vyžadují zprávy, které mají být zpracovány konkrétním správcem front nebo v určité posloupnosti. Takové žádosti mají

mít spřízněnosti. Možná budete muset upravit aplikace dříve, než je budete moci používat ve složitých klastrech.

- Můžete se rozhodnout použít volbu MQOO_BIND_ON_OPEN na serveru MQOPEN k vynucení odeslání zpráv do určitého cíle. Není-li správce cílové fronty k dispozici, zprávy nebudou doručeny, dokud nebude správce front opět dostupný. Zprávy nejsou směrovány do jiného správce front kvůli riziku duplikace.
- Je-li správce front hostitelem úložiště klastrů, je třeba znát jeho název hostitele nebo adresu IP. Tyto informace musíte zadat do parametru CONNAME , když vytvoříte definici CLUSSDR v ostatních správcích front, které se připojují ke klastru. Jestliže používáte DHCP, je IP adresa předmětem změny, protože DHCP může alokovat novou IP adresu pokaždé, když restartujete systém. Proto v definicích CLUSSDR nesmíte uvést adresu IP. I v případě, že všechny definice CLUSSDR určují název hostitele a nikoli adresu IP, definice by stále nebyly spolehlivé. DHCP neaktualizuje nutně záznam adresáře DNS pro hostitele s novou adresou. Je-li třeba jmenovat správce front jako úplná úložiště v systémech, které používají DHCP, nainstalujte software, který zaručuje, aby byl adresář DNS aktuální.
- Nepoužívejte generické názvy, například generické prostředky VTAM nebo Dynamic Domain Název Server (DDNS), jako názvy připojení pro kanály. Pokud se tak stane, mohou se kanály připojovat k jinému správci front, než jste očekávali.
- Můžete získat zprávu pouze z lokální fronty klastru, ale můžete vložit zprávu do libovolné fronty v klastru. Pokud otevřete frontu pro použití příkazu MQGET , otevře správce front lokální frontu.
- Pokud nastavíte jednoduchý klastr WebSphere MQ , nemusíte měnit žádnou z vašich aplikací. Aplikace může pojmenovat cílovou frontu ve volání MQOPEN a nemusí vědět o umístění správce front. Pokud nastavíte klastr pro správu pracovní zátěže, musíte přezkoumat aplikace a upravit je podle potřeby.
- Aktuální data monitorování a stavu pro kanál nebo frontu lze zobrazit pomocí příkazů DISPLAY CHSTATUS a DISPLAY QSTATUS **runmqsc** . Informace o monitorování lze použít k usnadnění měření výkonu a stavu systému. Monitorování je řízeno atributy správce front, fronty a kanálu. Monitorování automaticky definovaných odesílacích kanálů klastru je možné s atributem správce front MONACLS .

Související pojmy

Klastry

Jak klastry fungují

“Porovnání klastrování a distribuovaných front” na stránce 158
Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

“Komponenty klastru” na stránce 160
Klastry se skládají z správců front, klastrovaných úložišť, kanálů klastru a front klastru.

“Správa klastrů produktu IBM WebSphere MQ” na stránce 181
Klastry IBM WebSphere MQ můžete vytvářet, rozšiřovat a udržovat.

Související úlohy

“Konfigurace klastru správce front” na stránce 156
Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

“Nastavení nového klastru” na stránce 181
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.

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 produktu WebSphere MQ lze modul listener spustit pomocí příkazu START LISTENER . V systémech WebSphere MQ for IBM i, Okna, UNIX and 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.

Postup

1. Spusťte inicializátor kanálu.

- Windows Linux UNIX

  IBM WebSphere MQ pro systémy Windows, systémy UNIX and 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** .

2. Spusťte modul listener kanálu.

- Windows

  IBM WebSphere MQ pro Windows
  Použijte buď program modulu listener kanálu poskytovaný produktem WebSphere MQ, nebo prostředky poskytované operačním systémem.

  Chcete-li spustit modul listener kanálu produktu WebSphere MQ , použijte příkaz RUNMQLSR . Příklad:

  ```
  RUNMQLSR -t tcp -p 1414 -m QM1
  ```

- Linux UNIX

  IBM WebSphere MQ v systémech UNIX and Linux
  Použijte buď program modulu listener kanálu poskytovaný produktem WebSphere MQ, nebo prostředky poskytované operačním systémem; například **inetd** pro komunikaci TCP.

  Chcete-li spustit modul listener kanálu produktu WebSphere MQ , použijte příkaz **runmqlsr** . Příklad:

  ```
  runmqlsr -t tcp -p 1414 -m QM1
  ```

  Chcete-li použít produkt **inetd** ke spuštění kanálů, nakonfigurujte dva soubory:

  a. Upravte soubor /etc/services. Musíte být přihlášeni 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 WebSphere MQ. Můžete změnit číslo portu, ale musí se shodovat s číslem portu uvedeným na konci odesílání.

  b. 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 WebSphere MQ .

Aktualizace se stanou aktivní poté, co produkt **inetd** znovu načte konfigurační soubory. Zadejte následující příkazy z ID uživatele root:

V systému AIX:

```
refresh -s inetd
```

V systému HP-UX:

```
inetd -c
```

V systému Solaris nebo Linux:

a. Vyhledejte ID procesu **inetd** pomocí příkazu:

```
ps -ef | grep inetd
```

b. Spusťte příslušný příkaz následujícím způsobem:

– Pro Solaris 9 a Linux:

```
kill -1 inetd processid
```

– Pro Solaris 10 nebo novější verze:

```
inetconv
```

Jak dlouho se uchovávají informace v úložištích správce front?

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

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

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

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

Poznámka: U velkých klastrů může být rušivý, pokud mnoho správců front automaticky znovu odešle všechny informace o sobě ve stejnou dobu. Viz “Aktualizace ve velkém klastru může ovlivnit výkon a dostupnost klastru.” na stránce 297.

Související pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 296

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

Správa klastrů produktu IBM WebSphere MQ

Klastry IBM WebSphere MQ můžete vytvářet, rozšiřovat a udržovat.

Podrobnosti o tom, jak spravovat klastry produktu IBM WebSphere MQ , najdete v následujících dílčích tématech:

Související pojmy

Klastry

Jak klastry fungují

“Porovnání klastrování a distribuovaných front” na stránce 158

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

“Komponenty klastru” na stránce 160

Klastry se skládají z správců front, klastrovaných úložišť, kanálů klastru a front klastru.

Související úlohy

“Konfigurace klastru správce front” na stránce 156

Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

“Nastavení nového klastru” na stránce 181

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.

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.

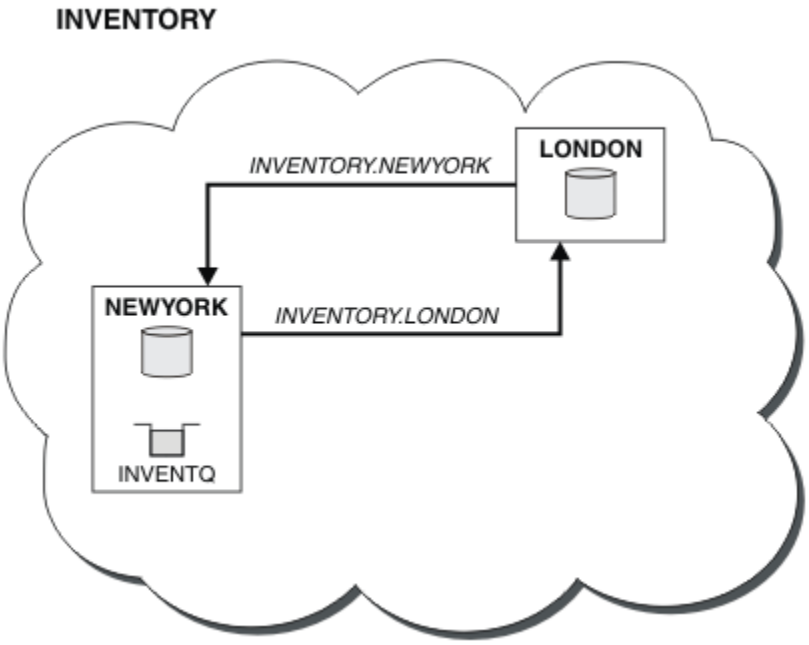
Než začnete

- Místo následujících pokynů můžete pomocí jednoho z průvodců dodávaných s produktem IBM WebSphere 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 fron**ta postupujte podle pokynů uvedených v průvodci.
- Informace o pozadí, které mohou pomoci pochopit kroky provedené při nastavení klastru, najdete v tématu “Fronty klastru” na stránce 162, Kanály a Listenery.

Informace o této úloze

Nastavujete novou síť IBM WebSphere 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 29 na stránce 182 ukazuje, jak tento klastr vypadá.



Obrázek 29. Klastr INVENTORY se dvěma správci front

Každý správce front v klastru, který se nenachází v systému z/OS , můžete nakonfigurovat tak, aby odesílal zprávy jiným správcům front v klastru s použitím různých přenosových front klastru.

Pokyny pro nastavení klastru 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 klastru pomocí protokolu TCP/IP s jedinou přenosovou frontou na správce front” na stránce 183
- “Nastavení klastru v systému TCP/IP s použitím více přenosových front na jednoho správce front” na stránce 185
- “Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 188
- “Ověření klastru” na stránce 190

Výsledky

Obrázek 29 na stránce 182 zobrazuje nastavení klastru INVENTORY pomocí této úlohy.

Je zřejmé, že INVENTORY je malý klastr. Nicméně je to užitečné jako důkaz konceptu. Důležitým krokem při pochopení tohoto klastru je rozsah, který nabízí pro budoucí vylepšení.

Související pojmy

Klastry

Jak klastry fungují

“Porovnání klastrování a distribuovaných front” na stránce 158
Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

“Komponenty klastru” na stránce 160
Klastry se skládají z správců front, klastrovaných úložišť, kanálů klastru a front klastru.

“Správa klastrů produktu IBM WebSphere MQ” na stránce 181
Klastry IBM WebSphere MQ můžete vytvářet, rozšiřovat a udržovat.

Související úlohy

“Konfigurace klastru správce front” na stránce 156
Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

Nastavení klastru pomocí protokolu TCP/IP s jedinou přenosovou frontou na správce front

Než začnete

- V systému AIX, HP-UX, IBM i, Linux, Solaris, and Windowsmusí být atribut správce front **DEFCLXQ**ponechán jako výchozí hodnota SCTQ.

Informace o této úloze

Chcete-li nastavit klastr v systému AIX, HP-UX, IBM i, Linux, Solaris, and Windows pomocí protokolu přenosu TCP/IP, postupujte takto.

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 191.

   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 WebSphere MQ for AIX.
   The responses vary on other platforms.
   ```

   c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštění 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)
   ```

   Poznámka: Definujete-li listener, mělo by být definováno číslo portu, používáte-li adresy IP v poli CONNAME a číslo portu není výchozím portem (1414). Příklad:

   ```
   DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(1415)
   ```

   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 definujte kanál příjemce klastru, v němž může správce front přijímat zprávy. 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 v 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'
   ```

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 .

   V každém správci front v klastru definujte jeden odesílací kanál klastru. Správce front odesílá zprávy do jednoho z správců front úplného úložiště v kanálu odesílatele klastru. V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich musí mít definici CLUSSDR , která 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 . Jakmile má 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.
```

8. 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')
```

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, and Windows 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 správcům front v klastru. Přidáte-li do klastru správce front, který má také používat různé přenosové fronty, postupujte podle úloh “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 193. Správce front v systému z/OS nelze nastavit tak, aby používal samostatné přenosové fronty klastru.

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 191.

   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 WebSphere MQ for AIX.
The responses vary on other platforms.
```

   c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštění 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 191 a “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 193.

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)
```

   Poznámka: Definujete-li listener, mělo by být definováno číslo portu, používáte-li adresy IP v poli CONNAME a číslo portu není výchozím portem (1414). Příklad:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(1415)
```

   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 definujte kanál příjemce klastru, v němž může správce front přijímat zprávy. 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 v 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'
```

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 .

   V každém správci front v klastru definujte jeden odesílací kanál klastru. Správce front odesílá zprávy do jednoho z správců front úplného úložiště v kanálu odesílatele klastru. V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich musí mít definici CLUSSDR , která 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 . Jakmile má 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. 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 191.

   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. 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 spuštění 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.

   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 definujte kanál příjemce klastru, v němž může správce front přijímat zprávy. 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)
   CONNAME(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)
   CONNAME(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)
   CONNAME(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 .

   V každém správci front v klastru definujte jeden odesílací kanál klastru. Správce front odesílá zprávy do jednoho z správců front úplného úložiště v kanálu odesílatele klastru. V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich musí mít definici CLUSSDR , která 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 . Jakmile má 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)
   CONNAME(CPIC) CLUSTER(INVENTORY)
   DESCR('LU62 Cluster-sender channel from LONDON to repository at NEWYORK')
   ```

   ```
   1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
   CONNAME(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)
   CONNAME(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( )
CONNAME(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)
CONNAME(192.0.2.1)             CURRENT
CHLTYPE(CLUSSDR)               STATUS(RUNNING)
RQMNAME(LONDON)
```

Odesílání zpráv mezi dvěma správci front pomocí produktu **amqsput**.

3. V systému LONDON spusťte příkaz **amqsput INVENTQ LONDON**.

   Zadejte některé zprávy, za nimiž bude následovat prázdný řádek.

4. V systému NEWYORK spusťte příkaz **amqsget 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:

- Klastr INVENTORY je nastaven tak, jak je popsáno v tématu “Nastavení nového klastru” na stránce 181. 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 klastru.
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 klastru, 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 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 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. Není třeba vytvářet definice pro ostatní správce front pro odeslání na přijímacím kanálu 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 PARISvytvořte následující definici pro kanál s názvem INVENTORY.LONDON ke správci front s adresou sítě 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')
   ```

4. Volitelné: Pokud se tento správce front znovu připojí ke klastru, proveďte některé další kroky navíc.

   a) Pokud přidáváte správce front do klastru, který byl dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:

      i) 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: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.

      ii) Restartujte kanál CLUSSDR (například pomocí příkazu START CHANNEL).

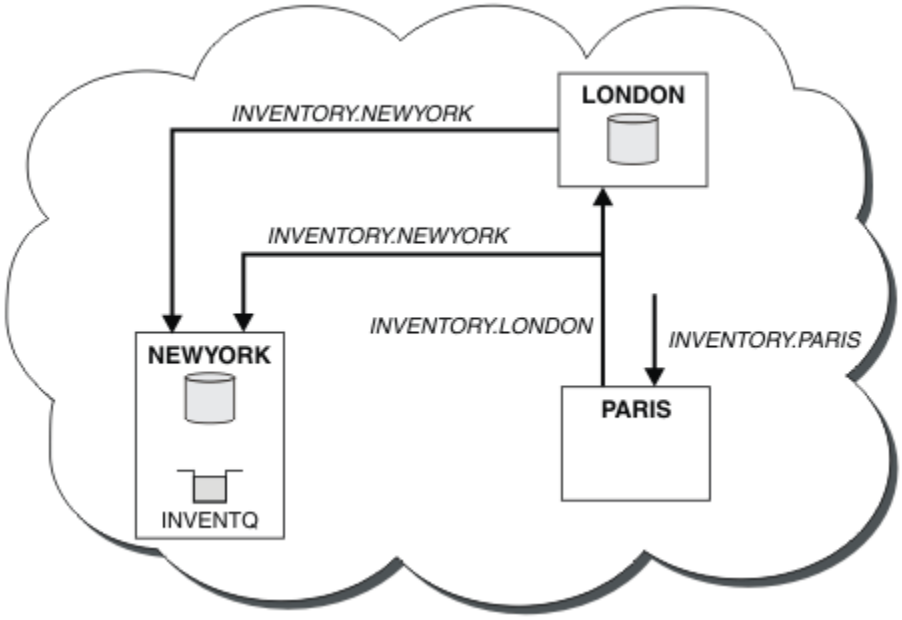
      iii) Restartujte kanál CLUSRCVR.

   b) Je-li klastr klastr publikování/odběru a znovu připojovaný správce front má odběry, zadejte následující příkaz, abyste se ujistili, že odběry proxy jsou správně synchronizovány v klastru:

      ```
      REFRESH QMGR TYPE(PROXYSUB)
      ```

Výsledky

Následující obrázek ukazuje klastr, který je nastaven touto úlohou.



Obrázek 30. 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 je definován na jiné platformě než z/OS.
- 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 181.

Informace o této úloze

Tato úloha je alternativou k produktu “Přidání správce front do klastru” na stránce 191, 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, použije 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 vyhrazené SYSTEM.CLUSTER.TRANSMIT.QUEUES se správcem front, který byl upgradován z dřívější verze produktu, ujistěte se, že SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE má volbu SHARE/NOSHARE nastavenou na **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: Proveďte 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. Není třeba vytvářet definice pro ostatní správce front pro odeslání na přijímacím kanálu klastru INVENTORY.PARIS. Další definice se automaticky provedou, když je třeba.

4. 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.

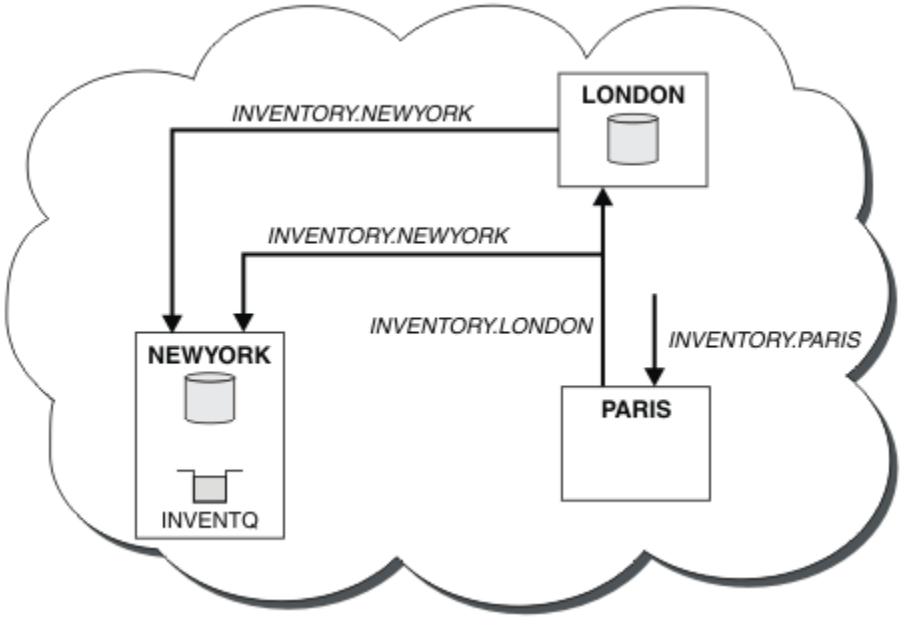
   V systému PARISvytvořte následující definici pro kanál s názvem INVENTORY.LONDON ke správci front s adresou sítě LONDON.CHSTORE.COM.

   ```
   DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at LONDON')
   ```

   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 31. 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 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 produktu Obrázek 37 na stránce 213 v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212 provedením kroků uvedených v této úloze.

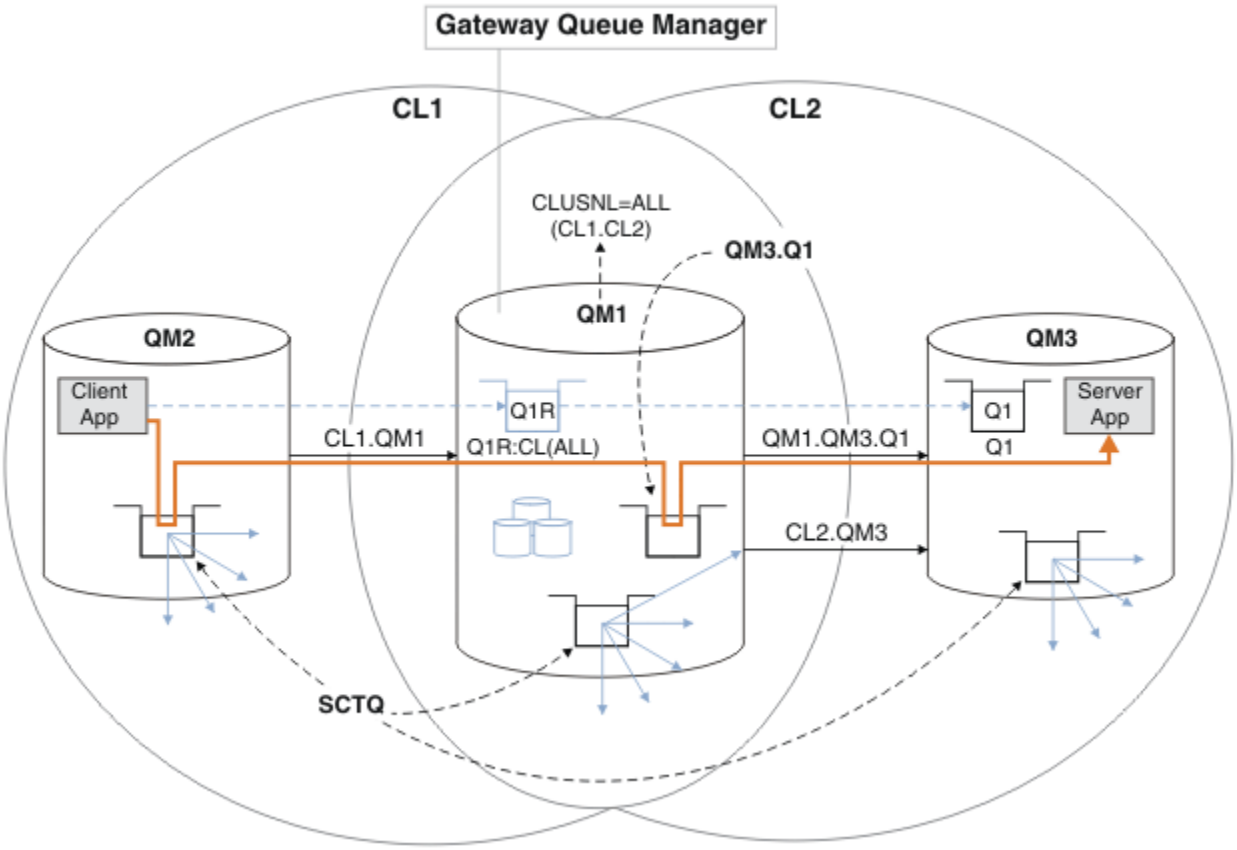
Informace o této úloze

Řešení používá distribuovanou frontu 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 32 na stránce 196je 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 správcích front. Chcete-li tuto nevýhodu překonat, viz “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198. Také musíte spravovat přepínač z jedné přenosové fronty do druhé.



Obrázek 32. Client-server aplikace implementovaná do rozbočovače a promluvila 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 **amqsput** na QM2 a zadejte zprávu.

```
C:\IBM\MQ>amqsput Q1R QM2
Sample AMQSPUT0 start
target queue is Q1R
Sample request message from QM2 to Q1 using Q1R

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 Q1R>
no more messages
Sample AMQSGET0 end
```

Související pojmy

"Řízení přístupu a více přenosových front klastru" na stránce 157
Zvolte mezi třemi režimy kontroly, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

"Klastrování: izolace aplikace pomocí více přenosových front klastru" na stránce 275
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

Související úlohy

"Přidání správce front do klastru: samostatné přenosové fronty" na stránce 193
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.

"Vytvoření dvou překrývajících se klastrů se správcem front brány" na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

"Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány" na stránce 195
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.

"Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv" na stránce 217
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 přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 198
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 201

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.

“Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

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.

Než začnete

1. Správce front brány musí být na serveru Version 7.5nebo novější a na jiné platformě než z/OS.
2. Sestavte překrývající se klastry zobrazené v produktu Obrázek 37 na stránce 213
   v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212
   provedením kroků uvedených v této úloze.

Informace o této úloze

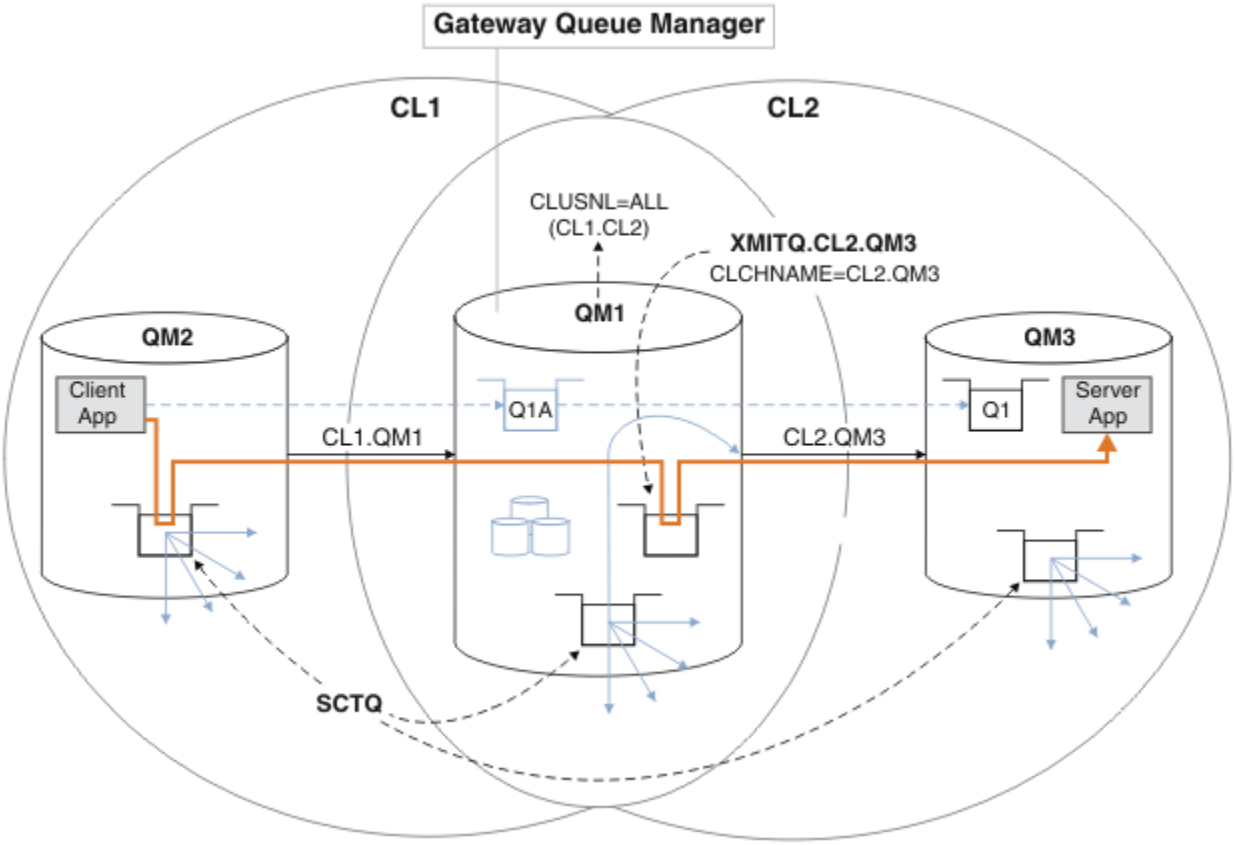
Na správci front brány, QM1, přidejte přenosovou frontu a nastavte její atribut fronty CLCHNAME. Nastavte parametr CLCHNAME na název přijímacího kanálu klastru v systému QM3, viz Obrázek 33 na stránce 199.

Toto řešení má řadu výhod oproti řešení popsanému v části “Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195:

- 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 33 na stránce 199 nevede k velké izolaci provozu jako konfigurace pomocí vzdálených front v produktu “Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195. 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 33 na stránce 199 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. Další informace naleznete v tématu “Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 201.



Obrázek 33. 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 WebSphere 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)
   CONNAME(127.0.0.1(1413))      CURRENT
   RQMNAME(QM3)                  STATUS(STOPPED)
   SUBSTATE(MQGET)               XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

c) Spusťte kanál, CL2.QM3.

```
*... On QM1
START CHANNEL(CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start WebSphere 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)
   CONNAME(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. Spusťte ukázkový program **amqsput** na QM2 , abyste vložili zprávu.

```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUT0 end
```

2. Spusťte ukázkový program **amqsget** , abyste získali zprávu z Q1 on 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

“Řízení přístupu a více přenosových front klastru” na stránce 157
Zvolte mezi třemi režimy kontroly, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru

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

“Přenosové fronty klastru a odesílací kanály klastru” na stránce 167
Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru.

Související úlohy

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 193
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.

“Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

“Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195
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.

“Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv” na stránce 217
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 přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198
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 201
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.

“Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

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 33 na stránce 199.

1. Správce front brány musí být na serveru Version 7.5nebo novější a na jiné platformě než z/OS.
2. Sestavte překrývající se klastry zobrazené v produktu Obrázek 37 na stránce 213
   v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212 provedením kroků uvedených v této úloze.

3. Postupujte podle kroků uvedených v části Obrázek 33 na stránce 199v části “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198 a vytvořte řešení bez dalšího klastru. Použijte jej jako základ pro kroky v této úloze.

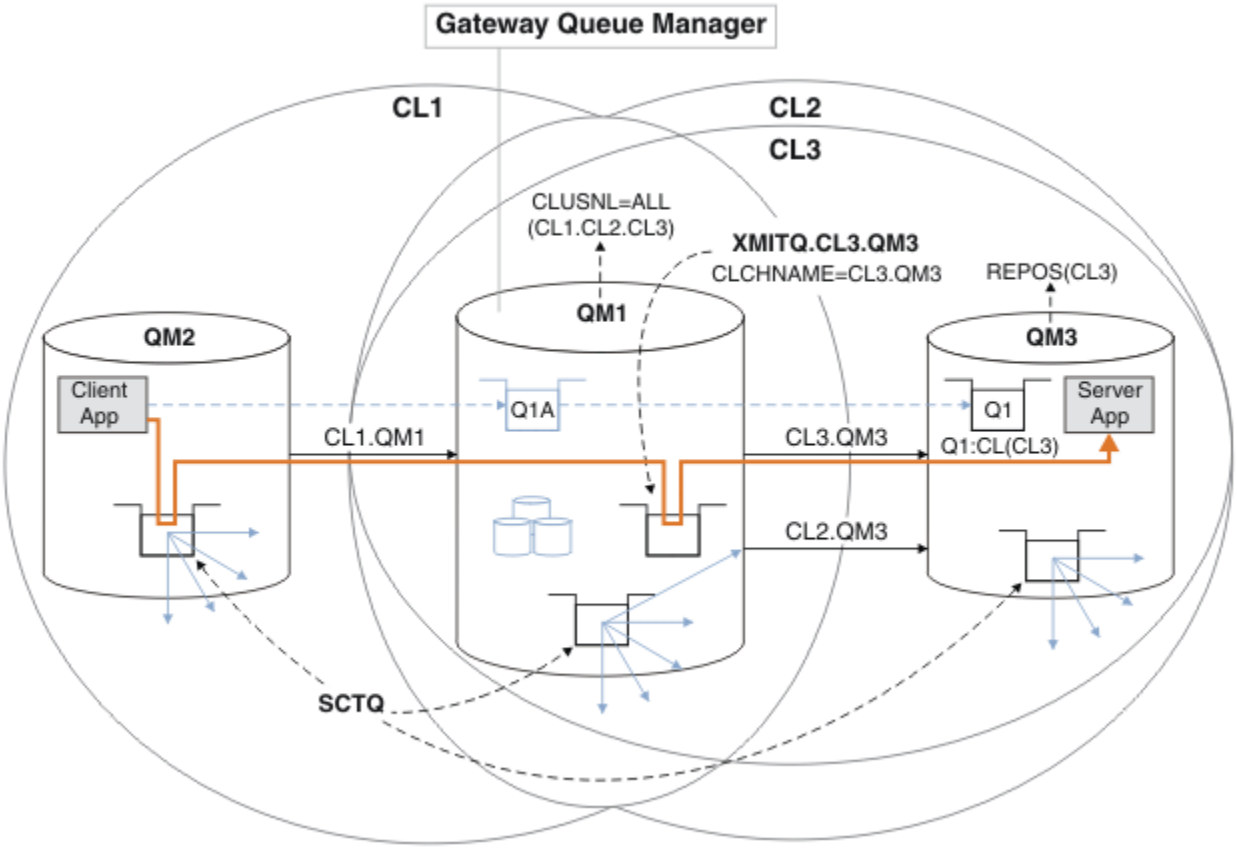
Informace o této úloze

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 198 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 198 přidáním klastru `CL3` za účelem izolace `Q1` na `QM3`. Aplikace budou pokračovat ve zpracování po celou dobu změny.

Nové a změněné definice jsou v produktu Obrázek 34 na stránce 203zvýrazněny. 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 WebSphere 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 198 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 34. 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(1415)') 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 fronty 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 přenese 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. Při odpovědi IBM WebSphere 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 WebSphere 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)
   CONNAME(127.0.0.1(1413))                CURRENT
   RQMNAME(QM3)                            STATUS(STOPPED)
   SUBSTATE(MQGET)                         XMITQ(XMITQ.CL2.QM3)
```

d) Spusťte kanál, CL2.QM3.

```
*... On QM1
START CHANNEL(CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start WebSphere 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)
   CONNAME(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 **amqsput** na QM2 , abyste vložili zprávu.

```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUT0 end
```

2. Spusťte ukázkový program **amqsget** , abyste získali zprávu z Q1 on 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

“Řízení přístupu a více přenosových front klastru” na stránce 157
Zvolte mezi třemi režimy kontroly, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

“Přenosové fronty klastru a odesílací kanály klastru” na stránce 167
Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru.

Související úlohy

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 193
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.

“Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

“Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195
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.

“Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv” na stránce 217
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 přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198
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 201

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.

“Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

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:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Nastavení nového klastru” na stránce 181. 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 vložením 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 WebSphere MQ o zjištění jména připojení ze systému, buď vynecháním CONNAME, nebo zadáním CONNAME(' '). IBM WebSphere MQ vygeneruje hodnotu CONNAME pomocí aktuální adresy IP systému; viz CONNAME. Není třeba vytvářet definice pro ostatní správce front pro odeslání na přijímacím kanálu 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 PARISvytvořte 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)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at LONDON')
   ```

4. Volitelné: Pokud se tento správce front znovu připojí ke klastru, proveďte některé další kroky navíc.
   a) Pokud přidáváte správce front do klastru, který byl dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:
      i) 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.

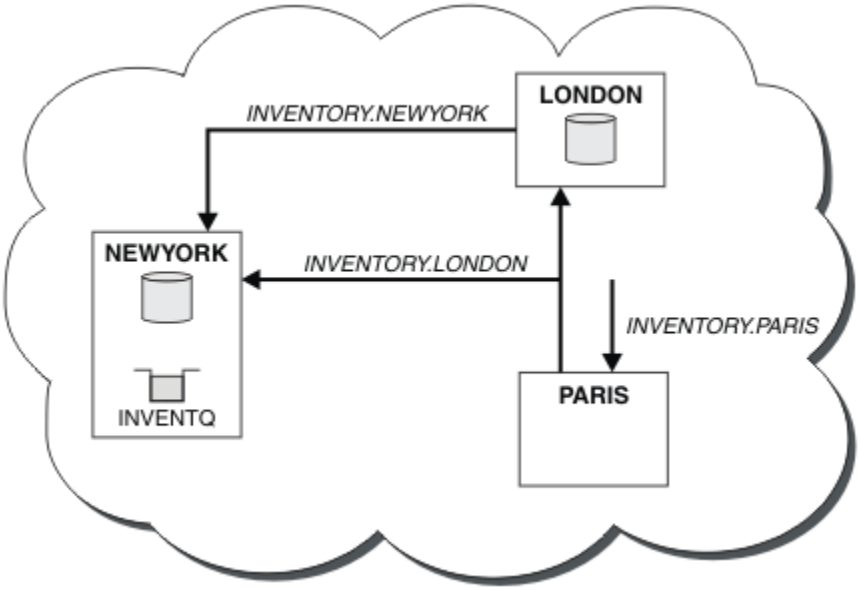
      ```
      REFRESH CLUSTER(INVENTORY) REPOS(YES)
      ```

      Poznámka: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.
      ii) Restartujte kanál CLUSSDR (například pomocí příkazu START CHANNEL).
      iii) Restartujte kanál CLUSRCVR.
   b) Je-li klastr klastr publikování/odběru a znovu připojovaný správce front má odběry, zadejte následující příkaz, abyste se ujistili, že odběry proxy jsou správně synchronizovány v klastru:

      ```
      REFRESH QMGR TYPE(PROXYSUB)
      ```

Výsledky

Klastr nastavený touto úlohou je stejný jako klastr pro “Přidání správce front do klastru” na stránce 191:



Obrázek 35. 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 WebSphere MQ interpretuje jako +QMNAME+ na název správce front (LONDON). IBM WebSphere MQ se pak shoduje s definicí kanálu s názvem INVENTORY.LONDON na odpovídající definici CLUSRCVR .

Produkt WebSphere MQ odešle zpět vyřešený název kanálu do správce front produktu PARIS . V systému PARISje 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 INVENTQ správce front NEWYORK. Když se aplikace hostovaná v systému v Paříži pokouší 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 odkazy

Definovat kanál

Přidání správce front, který je hostitelem fronty

Přidejte do klastru jiného správce front, aby bylo hostitelem jiné fronty produktu INVENTQ . Požadavky se odesílají střídavě do front v každém správci front. V existujícím hostiteli produktu INVENTQ 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:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 191. 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 doručením zpráv ve frontě INVENTQ .
- 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 224.

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 TORONTOdefinujte kanál CLUSRCVR :

   ```
   DEFINE CHANNEL(INVENTORY.TORONTO) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(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)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from TORONTO to repository at NEWYORK')
   ```
4. Volitelné: Pokud se tento správce front znovu připojí ke klastru, proveďte některé další kroky navíc.
   a) Pokud přidáváte správce front do klastru, který byl dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:
      i) 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: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.
      ii) Restartujte kanál CLUSSDR (například pomocí příkazu START CHANNEL).

iii) Restartujte kanál CLUSRCVR.

b) Je-li klastr klastr publikování/odběru a znovu připojovaný správce front má odběry, zadejte následující příkaz, abyste se ujistili, že odběry proxy jsou správně synchronizovány v klastru:

```
REFRESH QMGR TYPE(PROXYSUB)
```

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.

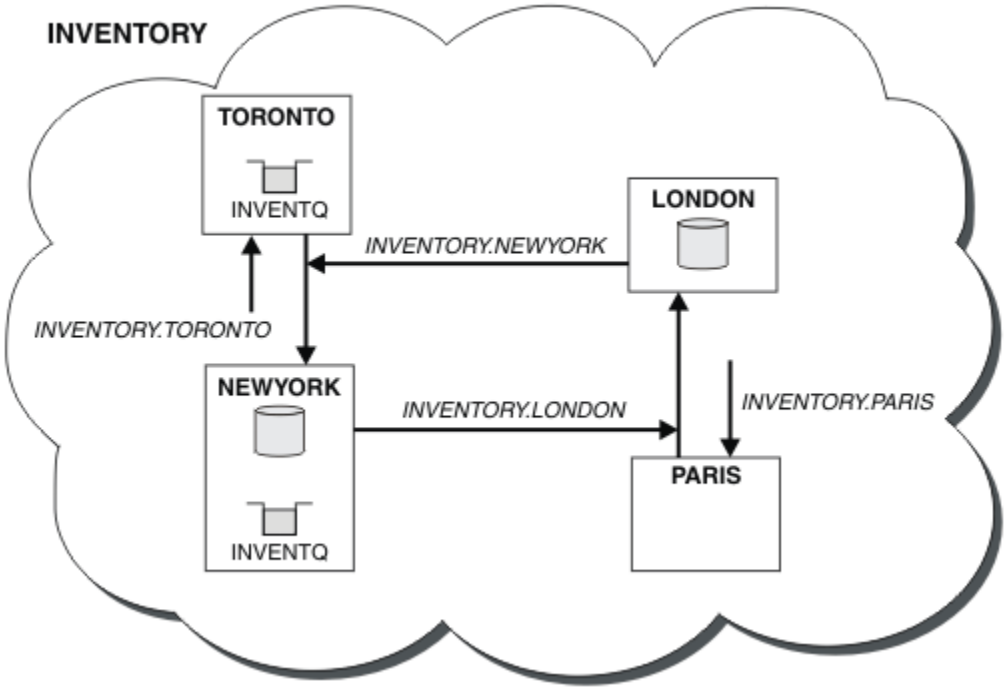
6. Definujte frontu klastru INVENTQ.

   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 36 na stránce 211 zobrazuje klastr INVENTORY , který je nastaven touto úlohou.



Obrázek 36. Klastr INVENTORY se čtyřmi správci front

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správcích front v klastru. 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 směrovány střídavě na TORONTO nebo NEWYORK, takže pracovní zátěž je vyvážená.

Tato úprava klastru byla dokončena, aniž byste museli měnit definice ve správcích front NEWYORK, LONDONa PARIS. Úplná úložiště v těchto správcích 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 klastru a zkontrolovat pole účtu ve všech zprávách a směrovat zprávy do příslušného správce front.

Jak pokračovat dále

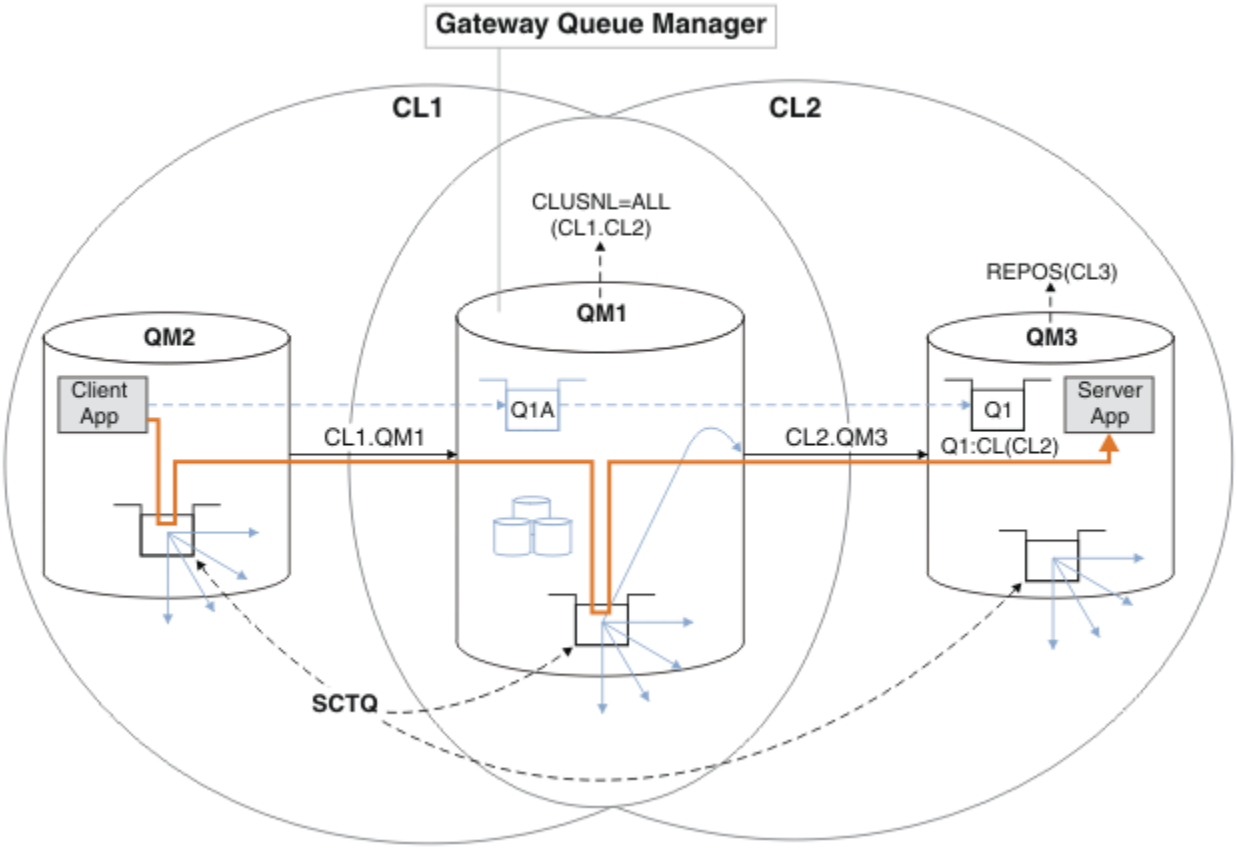
Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na systému IBM WebSphere MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front TORONTO. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

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 pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

Informace o této úloze

Příklad konfigurace klastru, který se používá k ilustraci izolování provozu zpráv klastru, je uveden v části Obrázek 37 na stránce 213. Příklad je popsán v části “Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275.



Obrázek 37. Aplikace klient-server implementovaná na centrální a paprskovou architekturu pomocí klastrů IBM WebSphere MQ

Aby byl počet kroků k vytvoření příkladu co nejméně, konfigurace je jednoduchá, spíše než realistická. Příklad může představovat integraci dvou klastrů vytvořených dvěma oddělenými organizacemi. Realističtější scénář viz “Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278.

Chcete-li vytvořit klastry, postupujte takto. Klastry se používají v následujících příkladech izolace přenosu zpráv z klientské aplikace do serverové aplikace.

Pokyny přidávají několik dalších správců front, aby měl každý klastr dvě úložiště. Správce front brány se z důvodů výkonu nepoužívá jako úložiště.

Postup

1. Vytvořte a spusťte správce front QM1, QM2, QM3, QM4, QM5.

```
crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE QMn
strmqm QmgrName
```

   Poznámka: QM4 a QM5 jsou záložní úplná úložiště pro klastry.

2. Definujte a spusťte moduly listener pro každého ze správců front.

```
*... On QMn
DEFINE LISTENER(TCP141n) TRPTYPE(TCP) IPADDR(hostname) PORT(141n) CONTROL(QMGR) REPLACE
START LISTENER(TCP141n)
```

3. Vytvořte seznam názvů klastrů pro všechny klastry.

```
*... On QM1
DEFINE NAMELIST(ALL) NAMES(CL1, CL2) REPLACE
```

4. Nastavte QM2 a QM4 úplná úložiště pro CL1, QM3 a QM5 úplná úložiště 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 odesílací a přijímací kanály klastru pro každého správce front a klastr.

   Spusťte následující příkazy v systémech QM2, QM3, QM4 a QM5, kde *c*, *n*a *m* mají hodnoty uvedené v části Tabulka 26 na stránce 214 pro každého správce front:

Tabulka 26. Hodnoty parametrů pro vytvoření klastrů 1 a 2

Správce front	**Klastr** ***c***	**Jiné úložiště** ***n***	**Toto úložiště** ***m***
QM2	1	4	2
QM4	1	2	4
QM3	2	5	3
QM5	2	3	5

```
*... On QMm
DEFINE CHANNEL(CLc.QMn) CHLTYPE(CLUSSDR)  CONNAME('localhost(141n)') CLUSTER(CLc) REPLACE
DEFINE CHANNEL(CLc.QMm) CHLTYPE(CLUSRCVR) CONNAME('localhost(141m)') CLUSTER(CLc) REPLACE
```

6. Přidejte správce front brány QM1do 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 správce front klastru Q1A do správce front brány.

```
*... On QM1
DEFINE QALIAS(Q1A)  CLUSNL(ALL) TARGET(Q1) TARGTYPE(QUEUE) DEFBIND(NOTFIXED) REPLACE
```

   Poznámka: Aplikace používající alias správce front ve všech ostatních správcích front, ale QM1, musí při otevírání alias fronty zadat hodnotu DEFBIND(NOTFIXED) . **DEFBIND** uvádí, zda jsou směrovací informace v záhlaví zprávy opraveny, když je fronta otevřena aplikací. Je-li nastavena na výchozí hodnotu OPEN, jsou zprávy směrovány na Q1@QM1. Produkt Q1@QM1 neexistuje, takže zprávy od jiných správců front skončí ve frontě nedoručených zpráv. Nastavením atributu fronty na hodnotu DEFBIND(NOTFIXED)se aplikace, jako např. **amqsput**, které standardně nastavují frontu na hodnotu **DEFBIND**, chovají správným způsobem.

9. Přidejte definice aliasů správce front klastru pro všechny správce front klastru 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 aliasů správce front v rámci zpráv přenosu správce front brány, které odkazují na správce front v jiném klastru. Viz téma Aliasy správců front s klastry.

Jak pokračovat dále

1. Otestujte definici aliasu fronty odesláním zprávy z QM2 do Q1 v QM3 pomocí definice aliasu fronty Q1A.
   a. Spusťte ukázkový program **amqsput** na QM2 , abyste vložili zprávu.

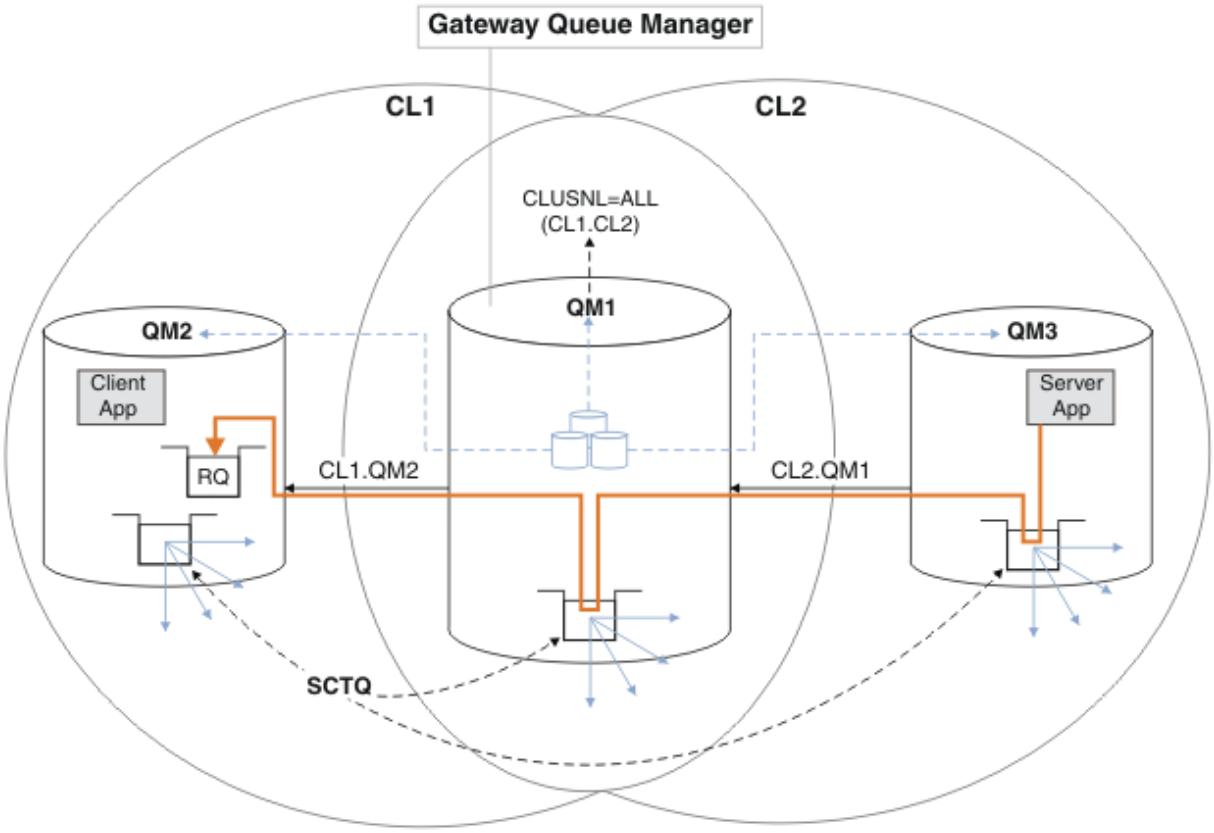
   ```
   C:\IBM\MQ>amqsput Q1A QM2
   Sample AMQSPUT0 start
   target queue is Q1A
   Sample request message from QM2 to Q1 using Q1A

   Sample AMQSPUT0 end
   ```

   b. Spusťte ukázkový program **amqsget** , abyste získali zprávu z Q1 on 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. Otestujte definice aliasů správce front odesláním zprávy požadavku a přijetím zprávy odpovědi ve frontě dočasných dynamických odpovědí.

   Diagram zobrazuje cestu, kterou zpráva odpovědi vede zpět do dočasné dynamické fronty s názvem RQ. Serverová aplikace připojená k produktu QM3otevře frontu odpovědí s použitím názvu správce front QM2. Název správce front QM2 je definován jako alias správce front klastru v systému QM1. QM3 směruje zprávu odpovědi na QM1. QM1 směruje zprávu na QM2.



Obrázek 38. Použití aliasu správce front k vrácení zprávy odpovědi do jiného klastru

Způsob, jakým směrování funguje, je následující. Každý správce front v každém klastru má v systému QM1definici aliasu správce front. Aliasy jsou klastrovány ve všech klastrech. Šedé čárkované šipky jednotlivých aliasů pro správce front ukazují, že každý alias správce front je převeden na skutečného

správce front alespoň v jednom z klastrů. V tomto případě je alias QM2 klastrován v klastru CL1 i CL2a je interpretován jako skutečný správce front QM2 v souboru CL1. Serverová aplikace vytvoří zprávu odpovědi s použitím názvu fronty pro odpověď RQa názvu správce front pro odpověď QM2. Zpráva je směrována do adresáře QM1 , protože definice aliasu správce front QM2 je definována v systému QM1 v klastru CL2 a správce front QM2 není v klastru CL2. Protože zprávu nelze odeslat do cílového správce front, je odeslána do správce front, který má definici aliasu.

QM1 umístí zprávu do přenosové fronty klastru na QM1 pro přenos do QM2. QM1 směruje zprávu do umístění QM2 , protože definice aliasu správce front v systému QM1 for QM2 definuje QM2 jako skutečného cílového správce front. Definice není kruhová, protože definice aliasů mohou odkazovat pouze na skutečné definice; alias nemůže ukazovat sám na sebe. Skutečnou definici interpretuje QM1, protože jak QM1 , tak QM2 jsou ve stejném klastru CL1. Produkt QM1 zjišťuje informace o připojení pro produkt QM2 z úložiště pro produkt CL1a směruje zprávu do adresáře QM2. Aby mohla být zpráva přesměrována produktem QM1, musí serverová aplikace otevřít frontu odpovědí s volbou DEFBIND nastavenou na MQBND_BIND_NOT_FIXED. Pokud serverová aplikace otevřela frontu odpovědí s volbou MQBND_BIND_ON_OPEN, zpráva nebude přesměrována a skončí ve frontě nedoručených zpráv.

a. Vytvořte klastrovanou frontu požadavků se spouštěčem na systému QM3.

```
*... On QM3
DEFINE QLOCAL(QR) CLUSTER(CL2) TRIGGER INITQ(SYSTEM.DEFAULT.INITIATION.QUEUE)
PROCESS(ECHO) REPLACE
```

b. Vytvořte definici aliasu fronty klastru QR ve správci front brány QM1.

```
*... On QM1
DEFINE QALIAS(QRA) CLUSNL(ALL) TARGET(QR) TARGTYPE(QUEUE) DEFBIND(NOTFIXED) REPLACE
```

c. Vytvořte definici procesu pro spuštění ukázkového programu echo **amqsech** na systému QM3.

```
*... On QM3
DEFINE PROCESS(ECHO) APPLICID(AMQSECH) REPLACE
```

d. Vytvořte modelovou frontu v systému 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 adresáře QM2 do adresáře QR v systému QM3 pomocí definice aliasu fronty QRA.

i) Spusťte program pro monitorování spouštěčů na systému QM3.

```
runmqtrm -m QM3
```

Výstup je

```
C:\IBM\MQ>runmqtrm -m QM3
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
01/02/2012  16:17:15: WebSphere MQ trigger monitor started.


_____________________________________________________
01/02/2012  16:17:15: Waiting for a trigger message
```

ii) Spusťte ukázkový program **amqsreq** na systému QM2 , abyste vložili požadavek a počkali 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 pojmy

“Řízení přístupu a více přenosových front klastru” na stránce 157
Zvolte mezi třemi režimy kontroly, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

Související úlohy

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 193
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.

“Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

“Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195
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.

“Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv” na stránce 217
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 přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198
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 201
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.

“Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

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.

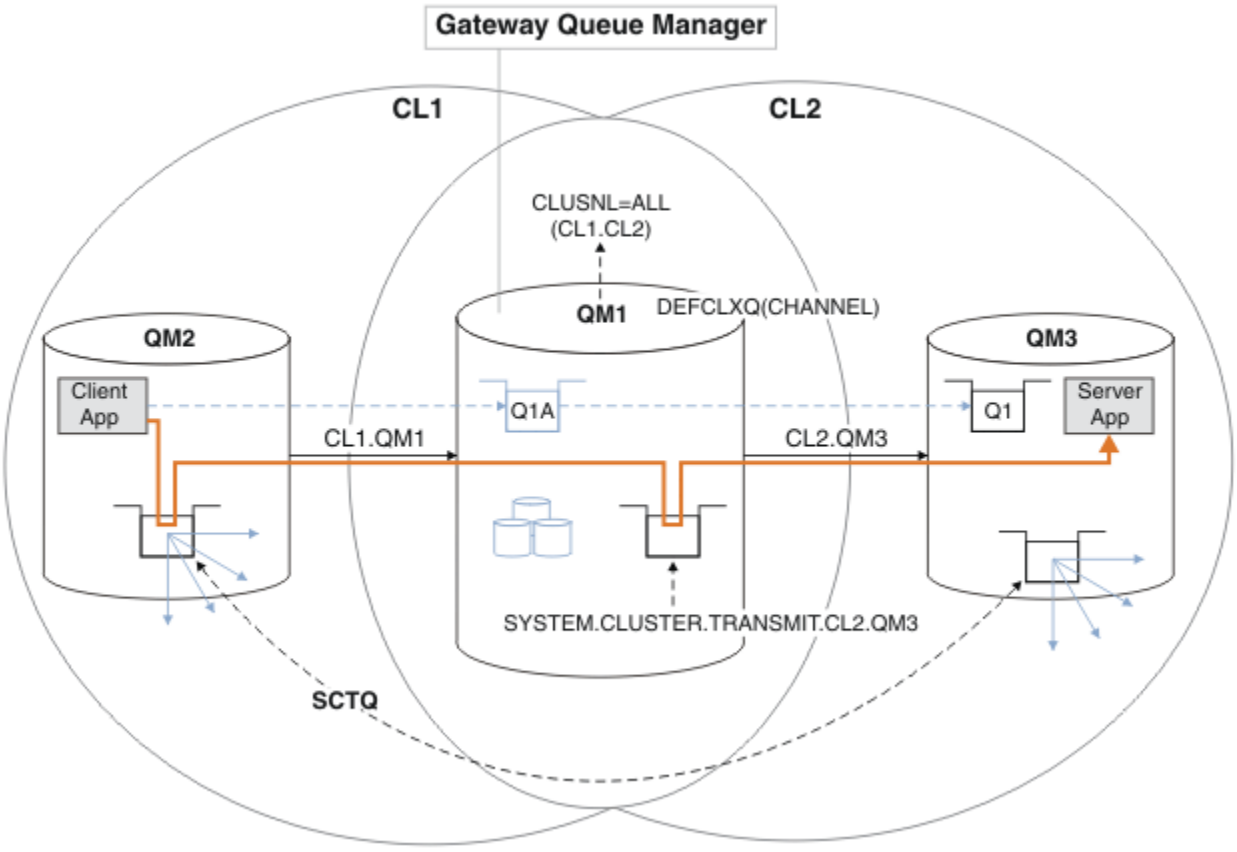
Než začnete

1. Správce front brány musí být na serveru Version 7.5nebo novější a na jiné platformě než z/OS.
2. Sestavte překrývající se klastry zobrazené v produktu Obrázek 37 na stránce 213 v produktu "Vytvoření dvou překrývajících se klastrů se správcem front brány" na stránce 212 provedením kroků uvedených v této úloze.

Informace o této úloze

Chcete-li implementovat architekturu s více frontami klastru, musí být správce front brány na serveru Version 7.5nebo 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 39 na stránce 218. 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 193.



Obrázek 39. 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)
      CONNAME(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)
      CONNAME(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)
      CONNAME(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)
      CONNAME(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 WebSphere 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)
      CONNAME(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)
      CONNAME(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)
   CONNAME(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)
   CONNAME(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 WebSphere 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)
   CONNAME(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)
   CONNAME(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)
   CONNAME(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)
   CONNAME(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. Spusťte ukázkový program **amqsput** na QM2 , abyste vložili zprávu.

   ```
   C:\IBM\MQ>amqsput Q1A QM2
   Sample AMQSPUT0 start
   target queue is Q1A
   Sample request message from QM2 to Q1 using Q1A

   Sample AMQSPUT0 end
   ```

   b. Spusťte ukázkový program **amqsget** , abyste získali zprávu z Q1 on 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 pojmy

“Řízení přístupu a více přenosových front klastru” na stránce 157
Zvolte mezi třemi režimy kontroly, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

Související úlohy

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 193
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.

“Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

“Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195

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.

“Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv” na stránce 217
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 přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198
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 201
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.

“Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

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:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front, který je hostitelem fronty” na stránce 209. 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 NEWYORKmají 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, OPPROCSa 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.TORONTOneobsahuje 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 TORONTOnejsou 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 TORONTOk 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, SALESa 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)
   ```

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 191.
- 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)
```

- Vyměňte všechny ostatní odesílací kanály klastru v klastru, které ukazují na LONDON s kanály, které ukazují na NEWYORK nebo PARIS. V tomto malém příkladu zde nejsou žádní další. Chcete-li zkontrolovat, zda jste zapomněli, zadejte příkaz DISPLAY CHANNEL z každého správce front zadáním příkazu 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.

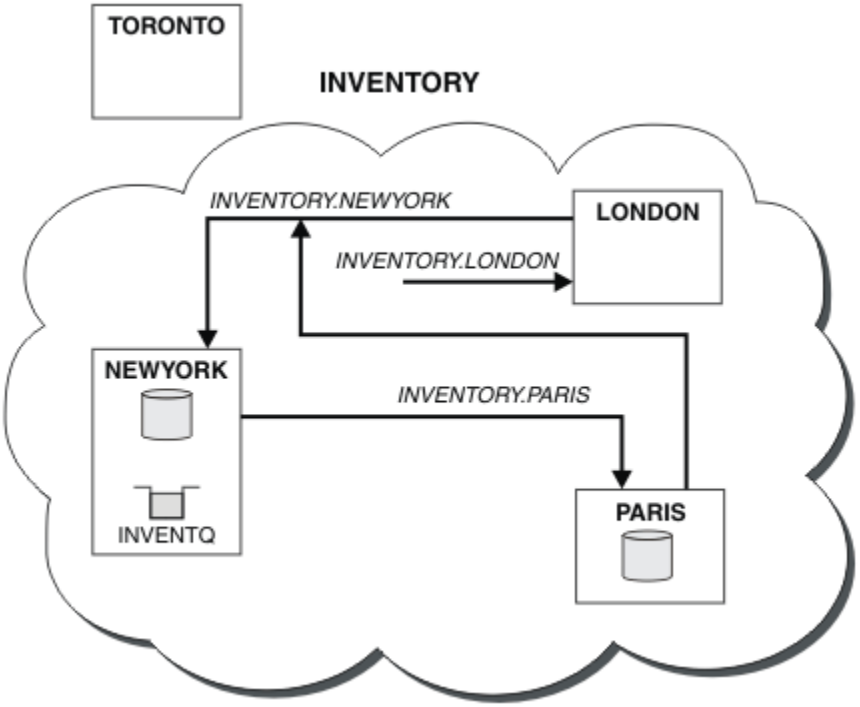
Poté, co produkt LONDON přestane být úplným úložištěm, pokud přijme takové požadavky, bude zapisovat chybové zprávy do svého protokolu chyb správce front. Následující příklady ukazují, které chybové zprávy se mohou zobrazit v produktu LONDON:

- 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 CLCLSDR opraveny tak, aby ukazovala na PARIS. Tato situace nesmí být tolerována jako platná konfigurace v dlouhodobém horizontu.

Výsledky

Obrázek 40 na stránce 226 zobrazuje klastr nastavený touto úlohou.



Obrázek 40. Klastr INVENTORY s úplným úložištěm byl přesunut do PARIS

Převod existující sítě na klastr

Převeďte existující distribuovanou síť front do klastru a přidejte dalšího správce front za účelem zvýšení kapacity.

Než začnete

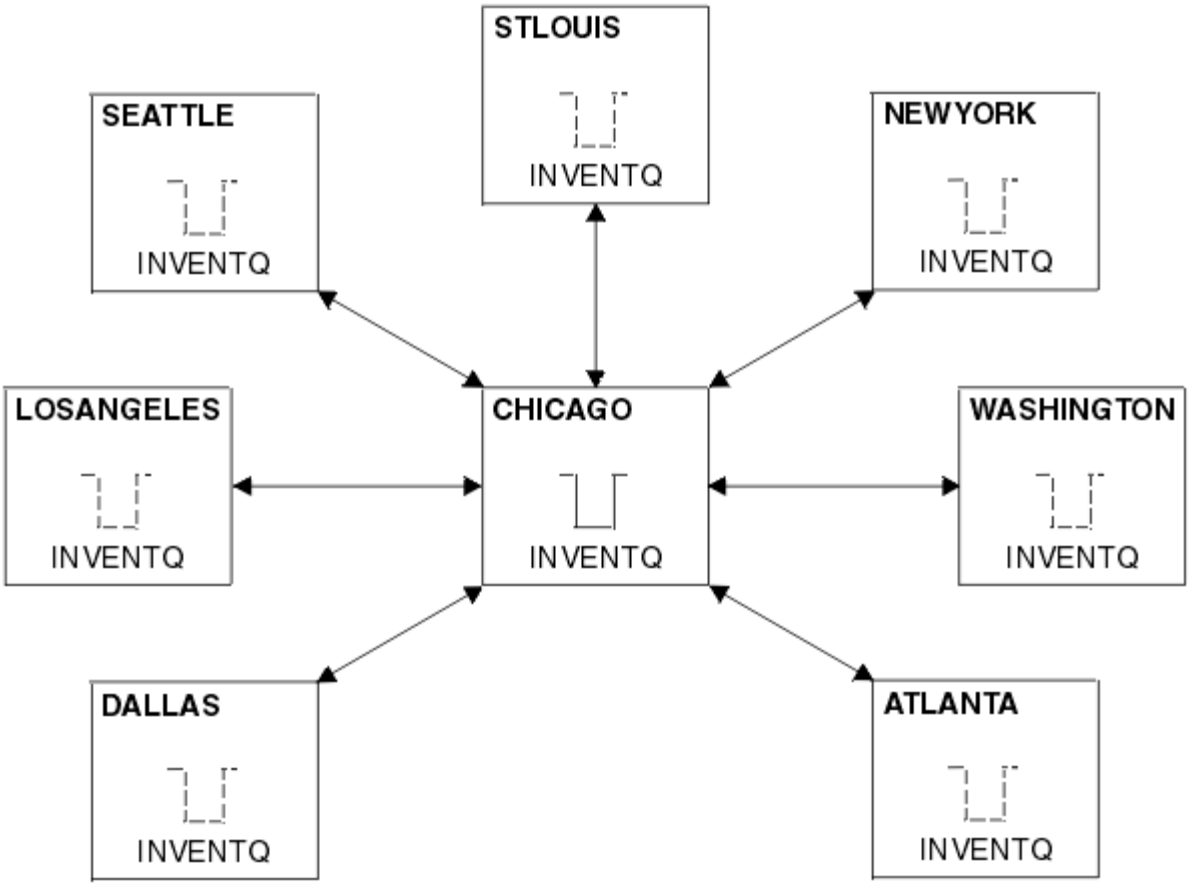
V produktu “Nastavení nového klastru” na stránce 181 prostřednictvím produktu “Přesunutí úplného úložiště do jiného správce front” na stránce 224 jste vytvořili a rozšířili nový klastr. Následující dva úlohy zkoumají odlišný přístup: převod existující sítě správců front na klastr.

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 WebSphere 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 doručením zpráv ve frontě `INVENTQ` , pro které má každý správce front definici vzdálené fronty.

  Tato síť je ilustrována v části Obrázek 41 na stránce 227.



Obrázek 41. 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 268

2. Upravte dva správce centrálních front, aby z nich učinili úplné správce front úložiště.

   Dva správci front CHICAGO a CHICAGO2 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 ATLANTAnapříklad:

   ```
   DEFINE CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(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 CHICAGO2:

   ```
   DEFINE CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(CHICAGO2.CHSTORE.COM) CLUSTER(CHNSTORE)
   DESCR('Cluster-sender channel to repository queue manager')
   ```

5. Nainstalujte aplikaci soupisu na CHICAGO2.

   You already have the inventory application on queue manager CHICAGO. Nyní je třeba vytvořit kopii této aplikace ve správci front CHICAGO2.

6. Definujte frontu INVENTQ v centrálních správcích front.

   V systému CHICAGOupravte definici lokální fronty pro frontu INVENTQ tak, aby byla fronta zpřístupněna pro klastr. Spusťte následující příkaz:

   ```
   ALTER QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
   ```

V systému CHICAGO2vytvořte definici pro stejnou frontu:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
```

V systému z/OSmůžete 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 INVENTQzjistí 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 klastr, 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:

- Klastr WebSphere MQ byl nastaven tak, jak je popsáno v tématu “Převod existující sítě na klastr” na stránce 227 .
- Je třeba implementovat nový klastr s názvem MAILORDER . Tento klastr se skládá ze čtyř správců front, kteří jsou v klastru CHNSTORE , CHICAGO, CHICAGO2 , SEATTLEa 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 klastr produktu MAILORDER se udržují na dvou správcích front CHICAGO a CHICAGO2.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li přidat nový propojený klastr, 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 klastry 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 klastr 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
```

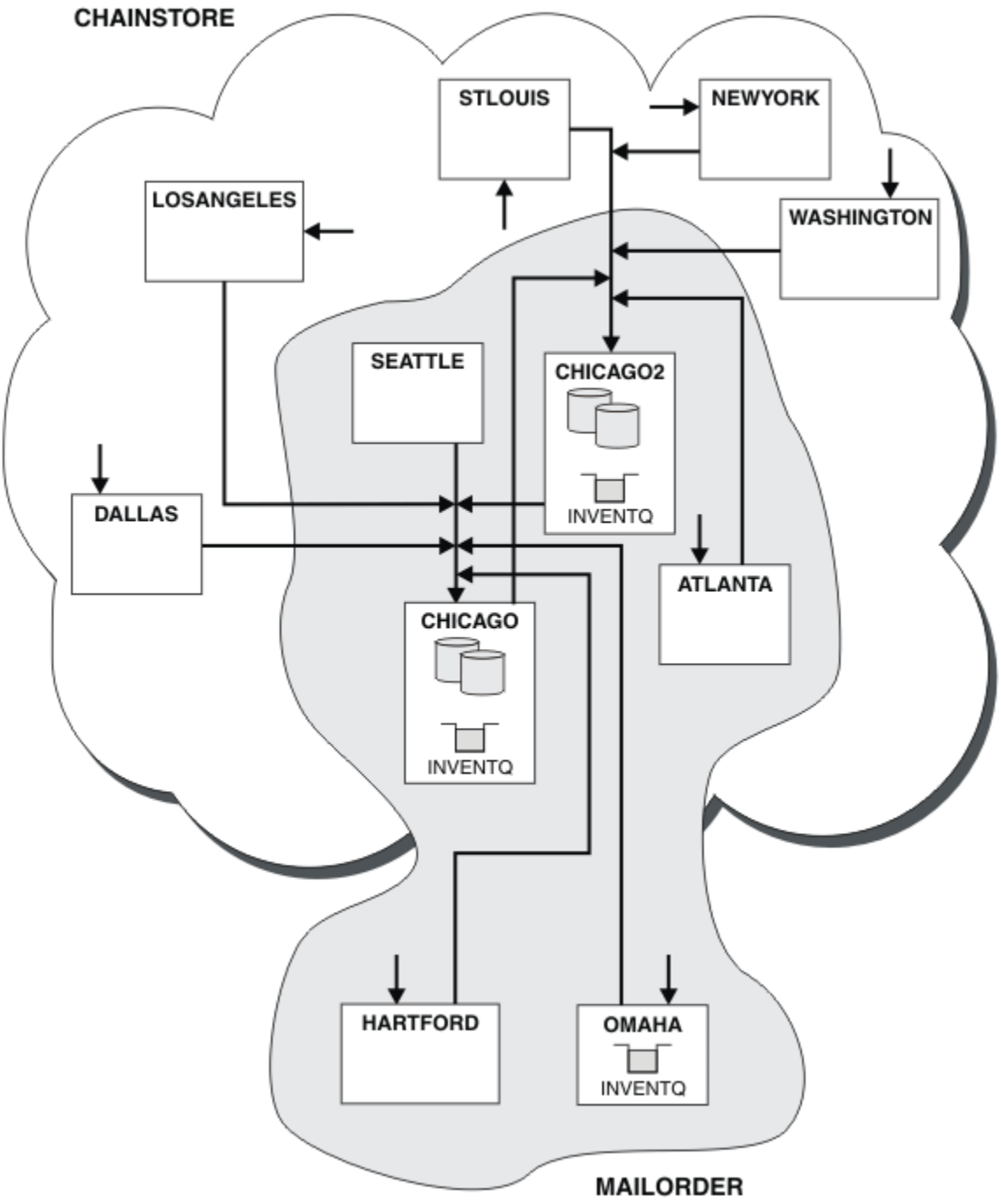
11.

Výsledky

Klastr, který je nastaven touto úlohou, se zobrazí v Obrázek 42 na stránce 232.

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 42. 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 nahraďte 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 změnily hodnotu atributu CLUSTER z produktu MAILORDER na hodnotu CHNSTORE. Například v HARTFORD zadejte:

```
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.

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 WebSphere MQ byl nastaven tak, jak je popsáno v tématu “Převod existující sítě na klastr” na stránce 227.
- 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. Spusťte následující příkaz:

   ```
   ALTER QLOCAL(INVENTQ) CLUSTER(' ')
   ```

   Když změníte frontu, informace v úplných úložištích se aktualizují a šíří po celém klastru. Aktivní aplikace používající produkt MQOO_BIND_NOT_FIXEDa aplikace používající MQOO_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 CHICAGO2upravte 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 CHNSTOREneexistují 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 238.

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.

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 236.

Před odebráním správce front z klastru se musíte ujistit, že správce front již není hostitelem prostředků potřebných pro klastr:

- Pokud správce front je hostitelem úplného úložiště, proveďte kroky 1-4 z produktu “Přesunutí úplného úložiště do jiného správce front” na stránce 224.
- Pokud správce front hostí fronty klastru, proveďte kroky 1 až 7 z produktu “Odebrání fronty klastru ze správce front” na stránce 222.
- Pokud správce front hostuje témata klastru, buď odstraňte témata (například pomocí příkazu DELETE TOPIC), nebo je přesuňte do jiných hostitelů.

  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.

Informace o této úloze

Tato vzorová úloha odstraní správce front LONDON z klastru INVENTORY . Klastr INVENTORY je nastaven tak, jak je popsán v části “Přidání správce front do klastru” na stránce 191, a upraven tak, jak je popsáno v tématu “Odebrání fronty klastru ze správce front” na stránce 222.

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. Upravte ručně definované kanály příjemce klastru tak, aby byly odebrány z klastru, ve správci front LONDON:

   ```
   ALTER CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) CLUSTER(' ')
   ```

2. 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.
3. 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 191. 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 238.

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 234.

Před odebráním správce front z klastru se musíte ujistit, že správce front již není hostitelem prostředků potřebných pro klastr:

- Pokud správce front je hostitelem úplného úložiště, proveďte kroky 1-4 z produktu “Přesunutí úplného úložiště do jiného správce front” na stránce 224.
- Pokud správce front hostí fronty klastru, proveďte kroky 1 až 7 z produktu “Odebrání fronty klastru ze správce front” na stránce 222.
- Pokud správce front hostuje témata klastru, buď odstraňte témata (například pomocí příkazu DELETE TOPIC), nebo je přesuňte do jiných hostitelů.

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.

Informace o této úloze

Tato vzorová úloha odstraní správce front LONDON z klastru INVENTORY . Klastr INVENTORY je nastaven tak, jak je popsán v části “Přidání správce front do klastru” na stránce 191, a upraven tak, jak je popsáno v tématu “Odebrání fronty klastru ze správce front” na stránce 222.

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 klastr hladce.

Postup

1. 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)
   ```

2. Sledujte stavy kanálů ve správci front LONDONaž 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.

3. Odstraňte ručně definované kanály klastru ve správci front LONDON:

   ```
   DELETE CHANNEL(INVENTORY.NEWYORK)
   DELETE CHANNEL(INVENTORY.TORONTO)
   ```

4. Zbývající správci front v klastru si stále uchovávají znalosti odebíraného 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 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)
```

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 191. 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 238.

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.

Důležité: Pokud odeberete správce front z klastru a aktualizujete jej pomocí REPOS (YES), nebudete jej moci znovu přidat jednoduše změnou atributu CLUSTER CLUSRCVR. Po změně atributu CLUSTER v parametru CLUSRCVR na hodnotu nonblank (tj. název klastru) bude navíc třeba aktualizovat klastr s REPOS (NO), kdy bude aktuální pořadová čísla na CLUSRCVR uvedena do aktuální doby. Poté bude správce front úspěšný, když se znovu zaváže do úplných úložišť a zbytku členů klastru. (Všimněte si, že verze příkazu REPOS (NO) musí být spuštěna poté, co byl kanál CLUSRCVR poskytnut správný název klastru.)

Toto omezení se vztahuje pouze na IBM WebSphere MQ Version 7.5 .

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 správci 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 234. Chcete-li odstranit informace o zbývajících členech klastru, zadejte ve správci 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 CLUSQMGR(*) CLUSTER(INVENTORY)
DISPLAY QCLUSTER(*) CLUSTER(INVENTORY)
DISPLAY TOPIC(*) CLUSTER(INVENTORY)
```

Související pojmy

Klastry

“Porovnání klastrování a distribuovaných front” na stránce 158
Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

“Komponenty klastru” na stránce 160
Klastry se skládají z správců front, klastrovaných úložišť, kanálů klastru a front klastru.

“Správa klastrů produktu IBM WebSphere MQ” na stránce 181
Klastry IBM WebSphere MQ můžete vytvářet, rozšiřovat a udržovat.

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.

   Produkt WebSphere MQ používá algoritmus vyrovnávání pracovní zátěže k určení toho, která místa určení jsou vhodná, namísto výběru lokálního správce front, je-li to možné.

a) Vynucení pozastavení správce front pomocí volby FORCE v příkazu SUSPEND QMGR :

```
SUSPEND QMGR CLUSTER(SALES) MODE(FORCE)
```

Produkt MODE(FORCE) vynutí zastavení všech příchozích kanálů od jiných správců front v klastru. Pokud nezadáte 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 správci front.

Údržba přenosové fronty klastru

Učinit veškeré úsilí, aby byly k dispozici přenosové fronty klastru. Jsou nezbytné pro výkon klastrů.

Než začnete

- Ujistěte se, že se přenosová fronta klastru nezaplní.
- 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 se nestává plnou.

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 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: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 296.

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 WebSphere MQ zajišťuje, že ve frontách nebudou ztracena žádná data.

Související pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 296
Příkaz **REFRESH CLUSTER** se používá k zahození všech lokálně uložených informací o klastru a znovusestavení těchto informací z úplných úložišť v klastru. Tento příkaz byste neměli používat, kromě výjimečných okolností. Pokud ji potřebujete použít, musíte zvážit, jak ji budete používat. Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

Obnova správce front

Pomocí příkazu REFRESH CLUSTER **runmqsc** převeďte 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: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům 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 pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 296
Příkaz **REFRESH CLUSTER** se používá k zahození všech lokálně uložených informací o klastru a znovusestavení těchto informací z úplných úložišť v klastru. Tento příkaz byste neměli používat, kromě výjimečných okolností. Pokud ji potřebujete použít, musíte zvážit, jak ji budete používat. Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

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 KAINT 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 zaplněn. 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, zařiďte, aby se kanál příjemce klastru ukončil a restartoval, když se kanál odesílatele klastru pokusí o restart.

  Na platformách jiných než z/OS
  Řídí problém konce příjemce klastru, který zůstává aktivní pomocí atributů AdoptNewMCA, AdoptNewMCATimeouta AdoptNewMCACheck v souboru qm.ini nebo v registru Windows NT .

Směrování zpráv do a z klastrů

Aliasy 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
Klastry
Jak klastry fungují
“Porovnání klastrování a distribuovaných front” na stránce 158
Porovnejte komponenty, které je třeba definovat pro připojení správců front používajících distribuované fronty a klastrování.

“Komponenty klastru” na stránce 160
Klastry se skládají z správců front, klastrovaných úložišť, kanálů klastru a front klastru.

“Správa klastrů produktu IBM WebSphere MQ” na stránce 181
Klastry IBM WebSphere MQ můžete vytvářet, rozšiřovat a udržovat.

“Aliasy správce front a klastry” na stránce 252
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 front a klastry” na stránce 254
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

“Aliasy fronty pro odpověď a klastry” na stránce 254
Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí lze použít s klastry stejně jako v prostředí distribuovaných front.

Související úlohy
“Konfigurace klastru správce front” na stránce 156
Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

“Nastavení nového klastru” na stránce 181

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 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.

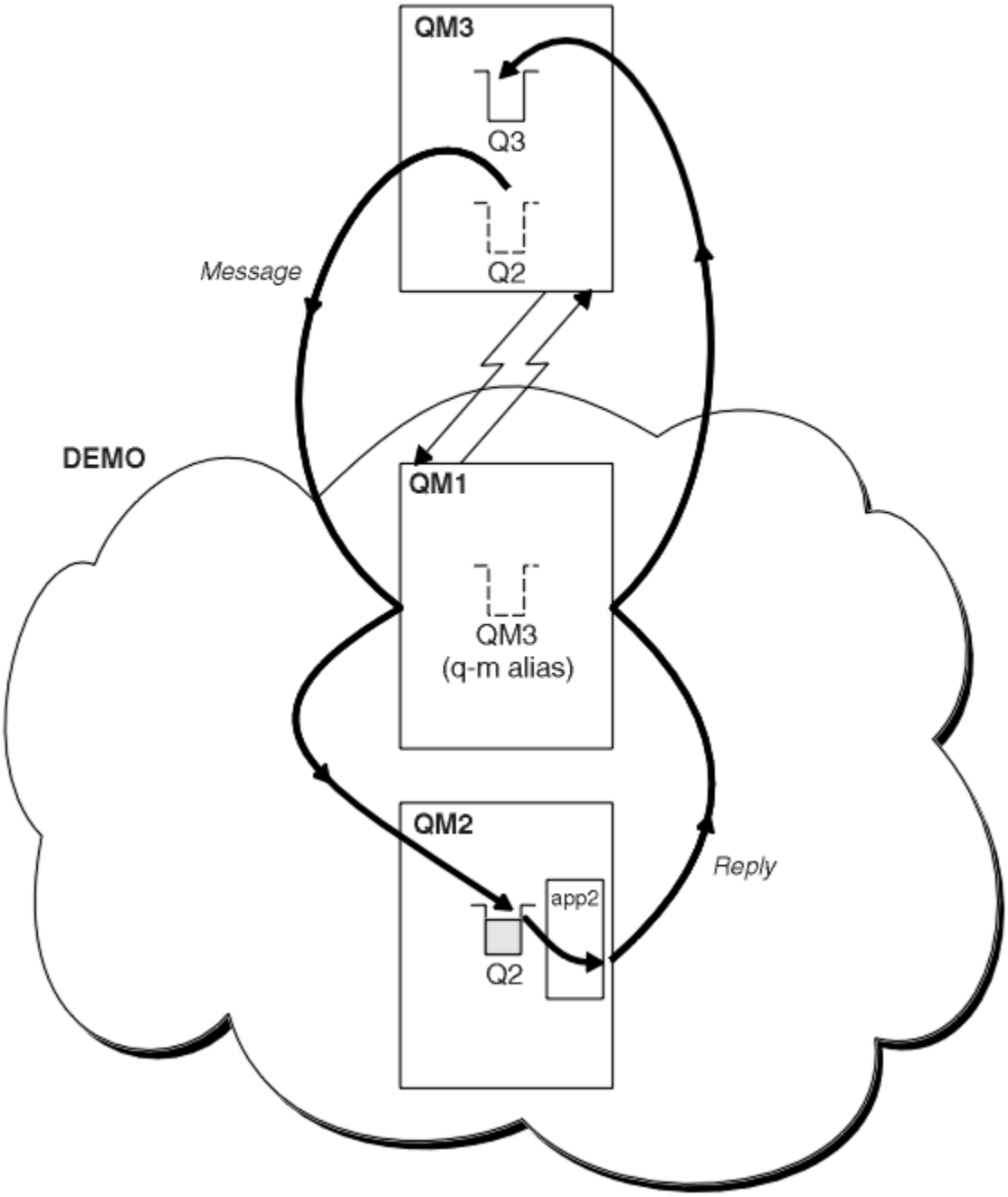
Než začnete

Produkt Obrázek 43 na stránce 244 zobrazuje správce front s názvem QM3 , který se nachází mimo klastr s názvem DEMO. QM3 může být správce front v produktu WebSphere 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 43. 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 umisťuje 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 43 na stránce 244.

V tomto příkladu aplikace v produktu QM3 vydá výzvu MQPUT k vložení zprávy do produktu Q2. Definice QREMOTE způsobí, že se zpráva bude směrována 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 odpovědí 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. WebSphere 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 odpovědí 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 odpovědí 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 ukázku poskytující jiný parametr obsahující alias fronty pro odpověď pro pojmenování alias správce front pro produkt `MQPUT`pro odpověď.

Související úlohy

“Skrytí názvu cílového správce front klastru” na stránce 246
Zasměrujte zprávu do fronty klastru, která je definovaná na libovolném správci front v klastru, aniž byste pojmenovali správce front.

Skrytí názvu cílového správce front klastru

Zasměrujte 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 246 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.

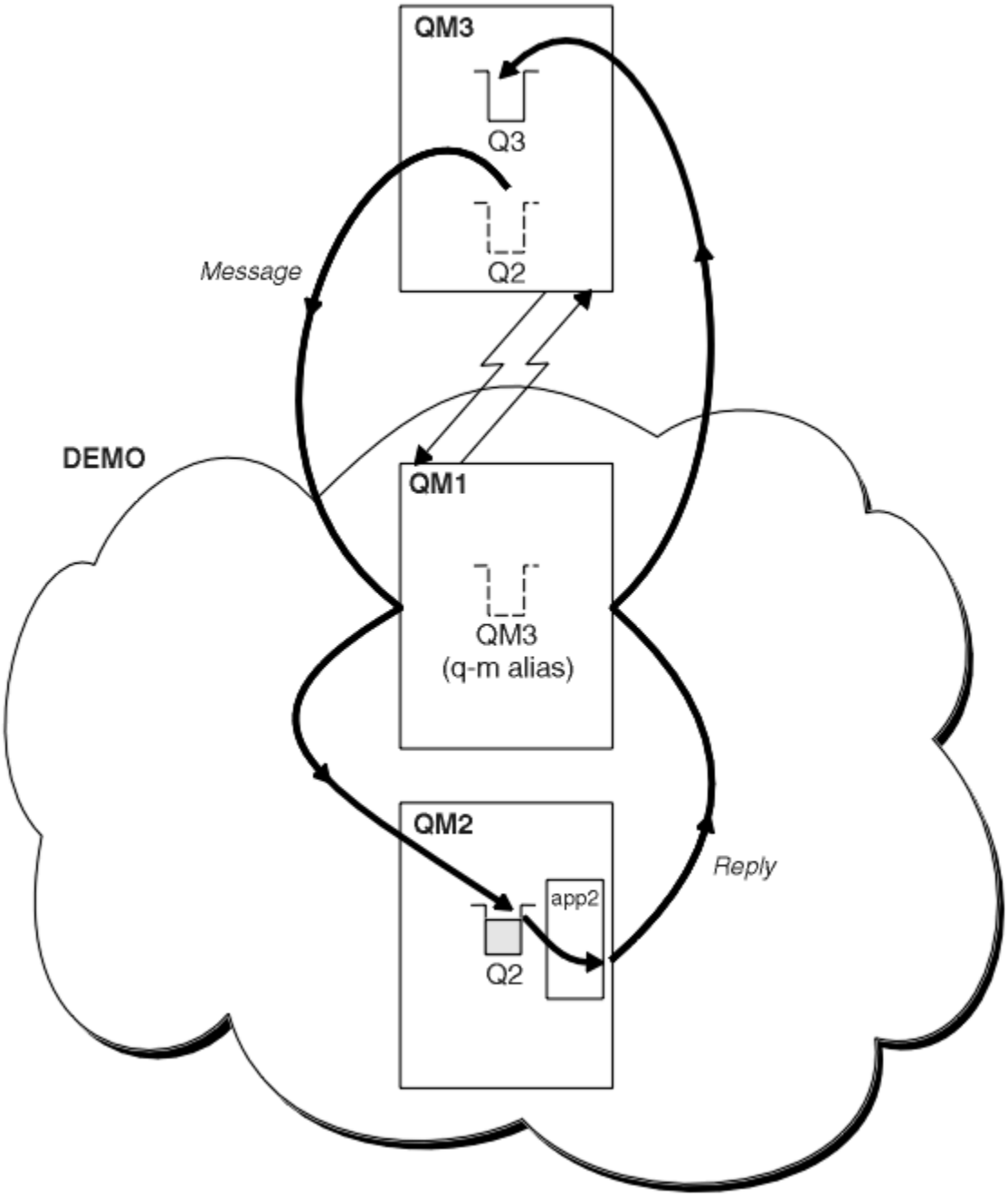
Informace o této úloze

Upravte úlohu “Konfigurace požadavku/odpovědi na klastr” na stránce 243tak, abyste skryli název cílového správce front v rámci klastru.

Postup

V tomto příkladu si prohlédněte téma Obrázek 44 na stránce 247 , definujte alias správce front ve správci front brány `QM1` s názvem `DEMO`:

```
DEFINE QREMOTE(DEMO) RNAME(' ') RQMNAME(' ')
```



Obrázek 44. 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 DEMOmísto toho, aby bylo nutné použít skutečné jméno správce front.

Pokud převezmou 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)
```

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 směruje zprávy do libovolného správce front v klastru, který je hostitelem fronty klastru Q2.

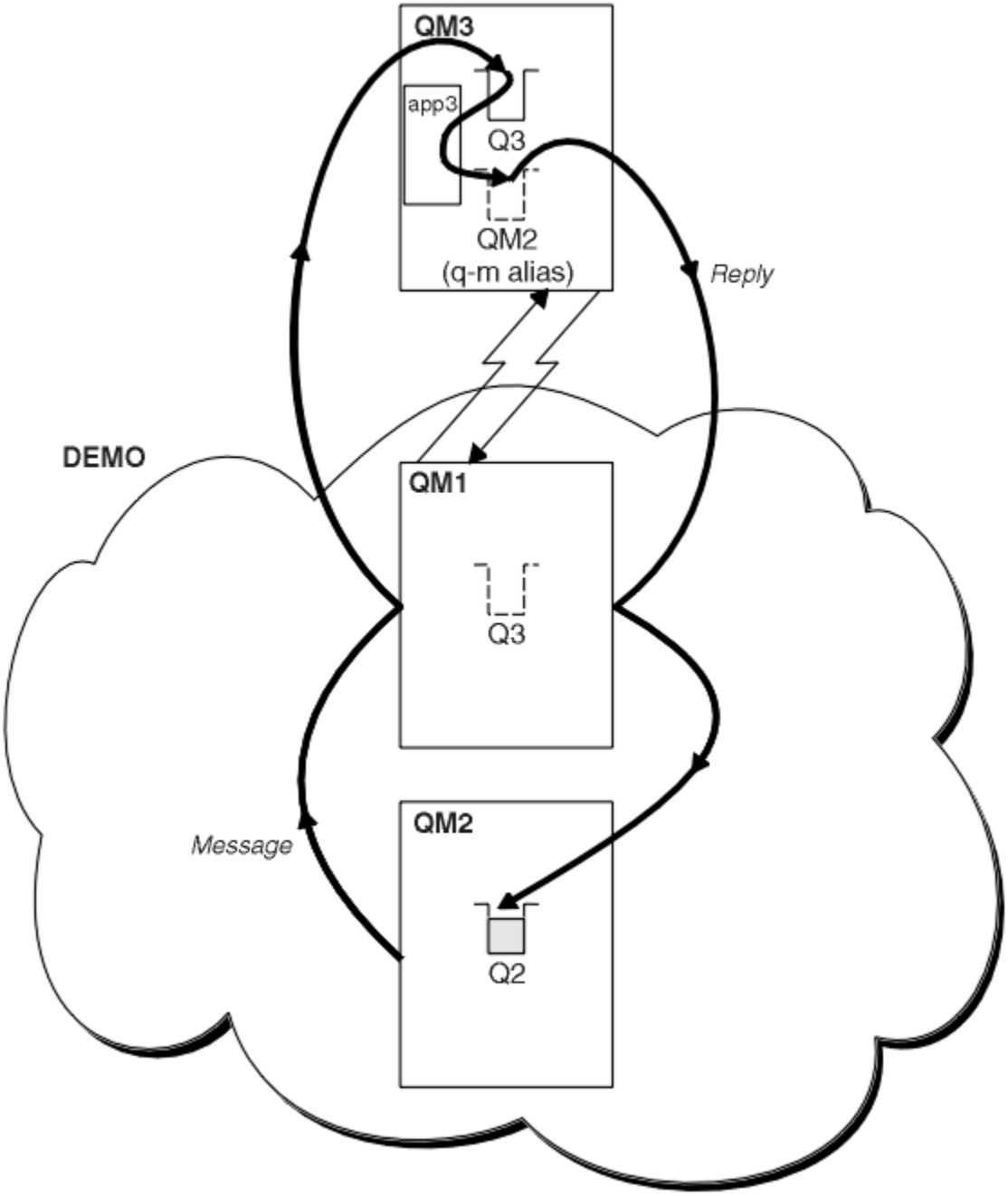
Konfigurace požadavku/odpovědi z klastru

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 45 na stránce 248 zobrazuje správce front QM2, uvnitř klastru DEMO. Odešle požadavek do fronty Q3, jehož hostitelem je správce front mimo klastr. Odpovědi jsou vraceny 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 45. 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 oznamuje 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 produktu Obrázek 45 na stránce 248.

   Aplikace v systému QM2 vydává volání MQPUT určující cílovou frontu a frontu, do níž mají být odesílány odpovědi. Cílová fronta je Q3 a fronta odpovědí 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.

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 tento příklad, jak ukazuje Obrázek 43 na stránce 244 v “Konfigurace požadavku/odpovědi na klastr” na stránce 243.

Informace o této úloze

V tomto scénáři správce front mimo klastr, QM3 v produktu Obrázek 46 na stránce 250odesílá požadavky do fronty Q2. Produkt Q2 je hostován na dvou správcích front v rámci klastru DEMO za účelem využití vyrovnávání pracovní zátěže. Fronta s názvem Q2 je definována ve správcích front QM2 a QM4 , ale nikoli ve správci front brány QM1. Požadavky z produktu QM3, správce front mimo klastr, se odesílají buď do instance produktu Q2.

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 46 na stránce 250.

Procedura rozšiřuje příklad v produktu Obrázek 43 na stránce 244 v produktu “Konfigurace požadavku/odpovědi na klastr” na stránce 243.

Postup

1. Definujte lokální frontu s názvem Q2 na každém z QM2 a QM4.

```
DEFINE QLOCAL(Q2) CLUSTER(DEMO) DEFBIND(NOTFIXED)
```

2. Vytvořte definici QREMOTE pro Q2 na QM3.

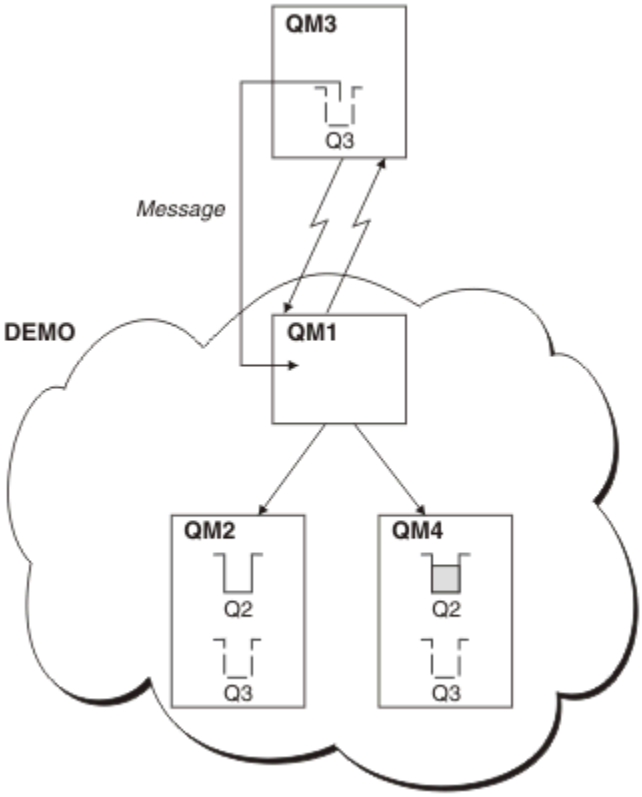
```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(Q3) XMITQ(QM1)
```

   Vytvořte definici QREMOTE pro každou frontu v klastru, do které produkt QM3 vkládá zprávy.
3. Vytvořte alias správce front Q3 v systému QM3.

```
DEFINE QREMOTE(Q3) RNAME(' ') RQMNAME(' ') CLUSTER(DEMO) DEFBIND(NOTFIXED)
```

   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 ' ' .
4. QM1, nemá správce front brány žádné speciální definice.

Výsledky



Obrázek 46. Vložení ze správce front mimo klastr

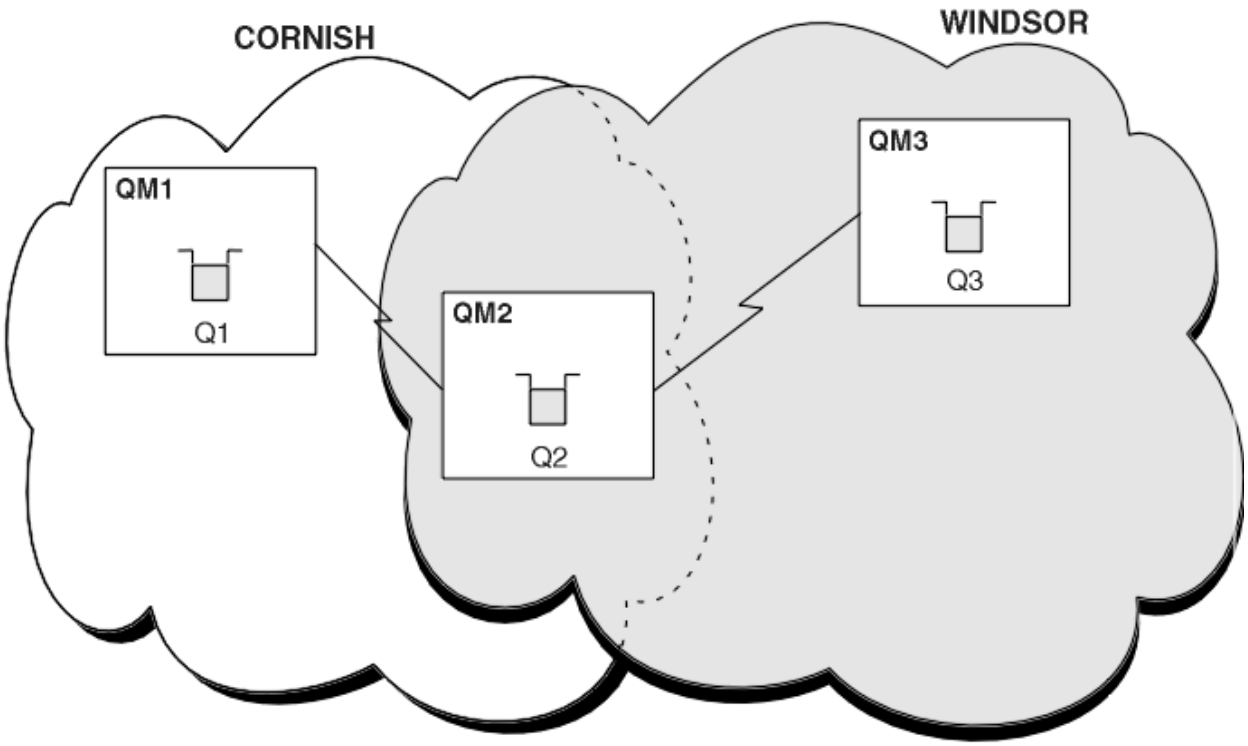
Když aplikace v QM3 vyvolá výzvu MQPUT k vložení zprávy do Q2, definice QREMOTE způsobí, že zpráva bude směrována přes správce front brány QM1. Produkt QM1 používá vyrovnávání pracovní zátěže k distribuci zpráv cílených na Q2 mezi frontami s názvem Q2 na dvou správcích front, QM2 a QM4, které mají aliasy správce front klastru pro produkt Q3.

Konfigurace cest zpráv mezi klastry

Připojte klastry pomocí správce front brány. Zviditelněte fronty nebo správce front pro všechny klastry definováním aliasů front klastru nebo správců front klastru ve správci front brány.

Informace o této úloze

Namísto seskupování všech správců front v jednom velkém klastru můžete mít mnoho menších klastrů. Každý klastr má v roli mostu jednoho nebo více správců front. Výhodou je, že můžete omezit viditelnost názvů front a správců front v rámci klastrů. Viz “Překrývání klastrů” na stránce 176. Použijte aliasy ke změně názvů front a správců front, abyste se vyhnuli konfliktům názvů nebo abyste dodrželi místní konvence pojmenování.



Obrázek 47. Přemostění mezi klastry

Obrázek 47 na stránce 251 zobrazuje dva klastry s mostem mezi nimi. Může být více než jeden most.

Nakonfigurujte klastry pomocí následujícího postupu:

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 on QM2, který bude obsahovat názvy obou klastrů.

```
DEFINE NAMELIST(CORNISHWINDSOR) DESCR('CornishWindsor namelist')
       NAMES(CORNISH, WINDSOR)
```

4. Definovat frontu klastru, Q2 na QM2

```
DEFINE QLOCAL(Q2) CLUSNL(CORNISHWINDSOR)
```

Jak pokračovat dále

QM2 je členem obou klastrů a je mostem mezi nimi. Pro každou frontu, kterou chcete zviditelnit přes most, potřebujete definici QALIAS na mostě. Například v systému Obrázek 47 na stránce 251v systému QM2potřebujete:

```
DEFINE QALIAS(MYQ3) TARGET(Q3) CLUSTER(CORNISH) DEFBIND(NOTFIXED)
```

Pomocí aliasu fronty může aplikace připojená ke správci front v adresáři CORNISH, například QM1, vložit zprávu do souboru Q3. Odkazuje na Q3 jako na MYQ3. Zpráva je směrována na Q3 v QM3.

Když otevřete frontu, musíte nastavit DEFBIND na hodnotu NOTFIXED nebo QDEF. Pokud je parametr DEFBIND ponechán jako výchozí, OPEN, správce front přeloží definici aliasu na správce front mostu, který je jeho hostitelem. Most zprávu nepředává.

Pro každého správce front, kterého chcete zviditelnit, potřebujete definici aliasu správce front. Například na systému QM2 potřebujete:

```
DEFINE QREMOTE(QM1) RNAME(' ') RQMNAME(QM1) CLUSTER(WINDSOR)
```

Aplikace připojená k libovolnému správci front v adresáři WINDSOR, například QM3, může vložit zprávu do libovolné fronty v systému QM1tak, že pojmenuje QM1 explicitně ve volání MQOPEN .

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 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 neklastrového 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 inzeruje 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 neklastlovými 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 soubor RQMNAME z definice aliasu správce front pro název správce front v záhlaví přenosu.

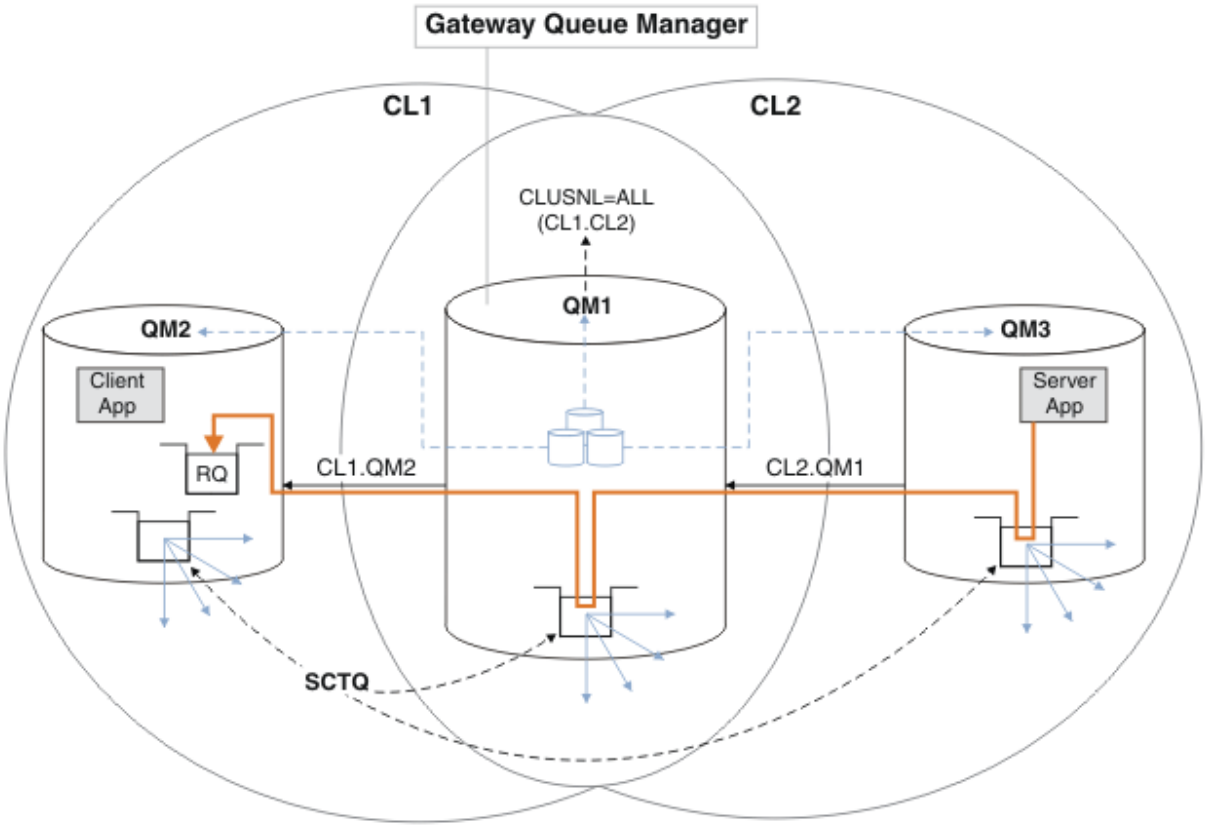
Existují dva důvody pro použití aliasu správce front tímto způsobem:

- Chcete-li směrovat 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 tématu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212, ze kterého je převzato tok zpráv s odpovědí znázorněný na obrázku 1.

Diagram zobrazuje cestu, kterou zpráva odpovědi vede zpět do dočasné dynamické fronty s názvem RQ. Serverová aplikace připojená k produktu QM3otevře frontu odpovědí s použitím názvu správce front QM2. Název správce front QM2 je definován jako alias správce front klastru v systému QM1. QM3 směruje zprávu odpovědi na QM1. QM1 směruje zprávu na QM2.



Obrázek 48. Použití aliasu správce front k vrácení zprávy odpovědi do jiného klastru

Způsob, jakým směrování funguje, je následující. Každý správce front v každém klastru má v systému QM1definici aliasu správce front. Aliasy jsou klastrovány ve všech klastrech. Šedé čárkované šipky

jednotlivých aliasů pro správce front ukazují, že každý alias správce front je převeden na skutečného správce front alespoň v jednom z klastrů. V tomto případě je alias QM2 klastrován v klastru CL1 i CL2a je interpretován jako skutečný správce front QM2 v souboru CL1. Serverová aplikace vytvoří zprávu odpovědi s použitím názvu fronty pro odpověď RQa názvu správce front pro odpověď QM2. Zpráva je směrována do adresáře QM1 , protože definice aliasu správce front QM2 je definována v systému QM1 v klastru CL2 a správce front QM2 není v klastru CL2. Protože zprávu nelze odeslat do cílového správce front, je odeslána do správce front, který má definici aliasu.

QM1 umístí zprávu do přenosové fronty klastru na QM1 pro přenos do QM2. QM1 směruje zprávu do umístění QM2 , protože definice aliasu správce front v systému QM1 for QM2 definuje QM2 jako skutečného cílového správce front. Definice není kruhová, protože definice aliasů mohou odkazovat pouze na skutečné definice; alias nemůže ukazovat sám na sebe. Skutečnou definici interpretuje QM1, protože jak QM1 , tak QM2 jsou ve stejném klastru CL1. Produkt QM1 zjišťuje informace o připojení pro produkt QM2 z úložiště pro produkt CL1a směruje zprávu do adresáře QM2. Aby mohla být zpráva přesměrována produktem QM1, musí serverová aplikace otevřít frontu odpovědí s volbou DEFBIND nastavenou na MQBND_BIND_NOT_FIXED. Pokud serverová aplikace otevřela frontu odpovědí s volbou MQBND_BIND_ON_OPEN, zpráva nebude přesměrována a skončí 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 mechanizmu 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 249 .

Aliasy fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí 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'
ReplyToQMgr=''
```

- 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.

Aliasy front a klastry

Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

Definice QALIAS se používá k vytvoření aliasu, pod kterým má být fronta známa. Alias můžete vytvořit z několika příčin:

- Chcete začít používat jinou frontu, ale nechcete měnit své aplikace.
- Nechcete, aby aplikace znaly skutečný název fronty, do které vkládají zprávy.
- Můžete mít konvenci pojmenování, která se liší od té, kde je fronta definována.
- Vaše aplikace nemusí být autorizovány pro přístup ke frontě podle skutečného názvu, ale pouze podle jejího aliasu.

Vytvořte definici QALIAS ve správci front pomocí příkazu DEFINE QALIAS . Spusťte například příkaz:

```
DEFINE QALIAS(PUBLIC) TARGET(LOCAL) CLUSTER(C)
```

Příkaz inzeruje frontu s názvem PUBLIC pro správce front v klastru C. PUBLIC je alias, který se interpretuje jako fronta s názvem LOCAL. Zprávy odeslané do adresáře PUBLIC jsou směrovány do fronty s názvem LOCAL.

Můžete také použít definici aliasu fronty k vyřešení názvu fronty na frontu klastru. Spusťte například příkaz:

```
DEFINE QALIAS(PRIVATE) TARGET(PUBLIC)
```

Tento příkaz umožňuje správci front používat název PRIVATE pro přístup k frontě inzerované jinde v klastru s názvem PUBLIC. Protože tato definice neobsahuje atribut CLUSTER , vztahuje se pouze na správce front, který jej vytváří.

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 klony. Každý správce front je schopen spouštět stejné aplikace a mít lokální definice stejných front. Pracovní zátěž mezi správci front můžete rozložit tak, že budete mít několik instancí určité aplikace. Každá instance aplikace přijímá zprávy a pracuje nezávisle na sobě.

Výhody použití klastrů tímto způsobem:

- Zvýšená dostupnost front a aplikací
- Rychlejší propustnost zpráv
- Více rovnoměrně rozložením pracovní zátěže ve vaší síti

Každý správce front, který je hostitelem instance určité fronty, může zpracovávat zprávy určené pro danou frontu. Aplikace nepojmenujte správce front při odesílání zpráv. Algoritmus správy pracovní zátěže určuje, který správce front tuto zprávu zpracovává.

Další informace o konfiguracích klastru pro správu pracovní zátěže naleznete v následujících dílčích tématech:

Související pojmy

Klastry

Jak klastry fungují

“Porovnání klastrování a distribuovaných front” na stránce 158

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

“Komponenty klastru” na stránce 160

Klastry se skládají z správců front, klastrovaných úložišť, kanálů klastru a front klastru.

“Správa klastrů produktu IBM WebSphere MQ” na stránce 181
Klastry IBM WebSphere MQ můžete vytvářet, rozšiřovat a udržovat.

“Směrování zpráv do a z klastrů” na stránce 242
Aliasy 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 156
Pomocí odkazů v tomto tématu zjistíte, jak fungují klastry, jak navrhnout konfiguraci klastru, a jak nastavit jednoduchý klastr.

“Nastavení nového klastru” na stránce 181
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.

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.

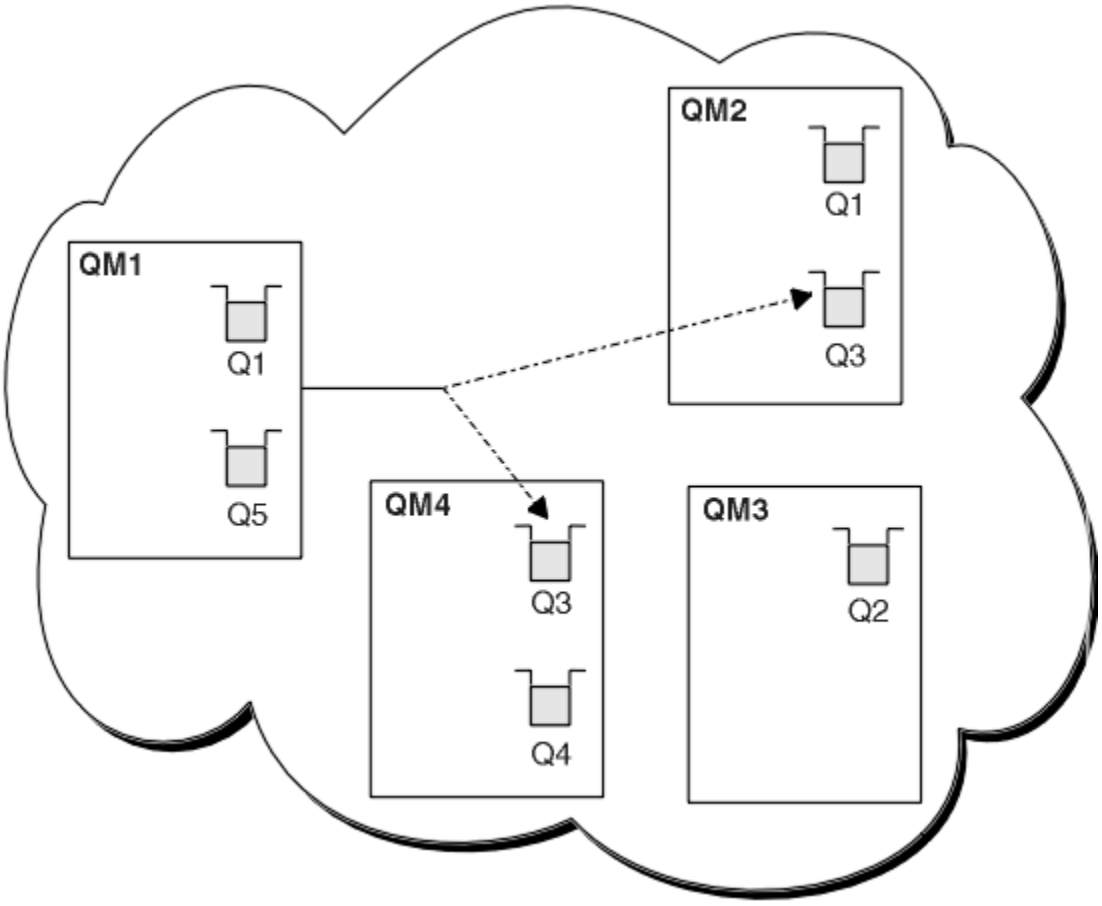
Obrázek 49 na stránce 257 ukazuje klastr, v němž je pro frontu Q3více než jedna definice. Pokud aplikace v produktu QM1 vloží zprávu do produktu Q3, nemusí nutně vědět, která instance produktu Q3 bude zpracovávat svou zprávu. Je-li aplikace spuštěna na serveru QM2 nebo v produktu QM4, , kde jsou lokální 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 správci 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 přesměrována. Nejsou-li k dispozici žádné instance fronty, bude zpráva umístěna do fronty nedoručených zpráv.



Obrázek 49. Klastr s více instancemi stejné fronty.

Jedním z faktorů, které mohou zabránit přesměrování zpráv, je, že zprávy byly přiřazeny k opravenému správci front nebo kanálu s volbou MQBND_BIND_ON_OPEN. Zprávy, které jsou svázány s produktem MQOPEN , nejsou nikdy znovu přiděleny jinému kanálu. Všimněte si také, že k opětovnému přidělení zpráv dochází pouze tehdy, když se kanál klastru skutečně nedaří. K opětovné alokaci nedojde v případě, že kanál již selhal.

Systém se pokusí přesměrovat 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 přesměrována.

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:

- Klastr 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 doručením 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 viz “Práce s afinitními zprávami” na stránce 268.

3. Instalovat inventární aplikaci na systém v Paříži.
4. Definujte frontu klastru INVENTQ.

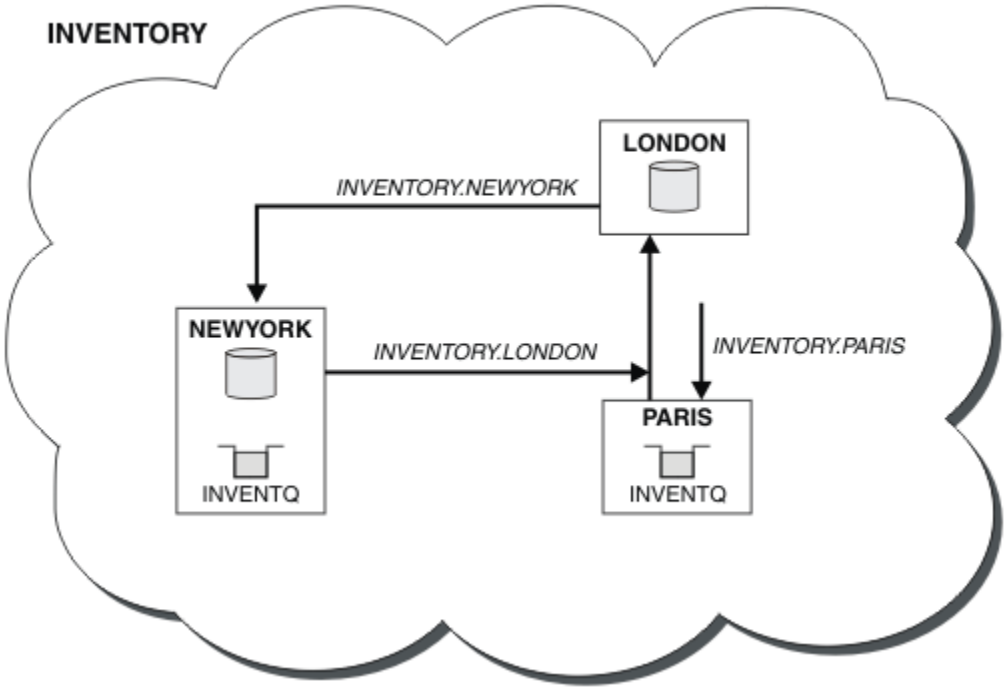
   Frontu INVENTQ , která je již hostována správcem front NEWYORK , je také hostována pomocí PARIS. Definujte jej ve správci front produktu PARIS takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte iniciátor kanálu na produktu WebSphere MQ pro 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 50 na stránce 258 zobrazuje klastr nastavený touto úlohou.



Obrázek 50. Klastr INVENTORY se třemi správci front

Úpravy tohoto klastru byly provedeny bez změny správců front NEWYORK nebo LONDON. Úplná úložiště v těchto správcích 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 správcích 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.

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:

- Klastr 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 připojil 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)
   CONNAME('TOKYO.NETB.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
   channel using network B for TOKYO')
   ```

   ```
   DEFINE CHANNEL(INVENTORY.TOKYO.NETA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME('TOKYO.NETA.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
   channel using network A for TOKYO')
   ```
3. Definujte kanál CLUSSDR ve správci front TOKYO.

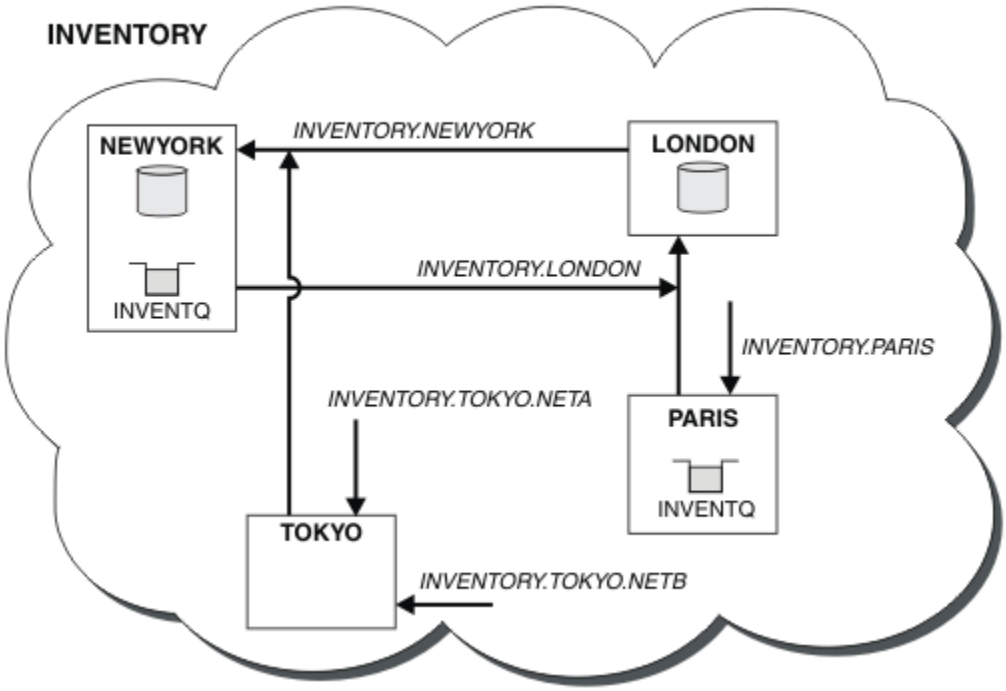
   Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK, takže TOKYO potřebuje následující definici:

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-sender
channel from TOKYO to repository at NEWYORK')
```

Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte iniciátor kanálu na produktu WebSphere MQ pro 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 51 na stránce 260 zobrazuje klastr nastavený touto úlohou.



Obrázek 51. 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 úlohy

“Přidání správce front do klastru” na stránce 191
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:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Použití dvou sítí v klastru” na stránce 259. 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 sítě, mohou používat sekundární sítě.

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 191. 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 .
- 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 CHICAGOdefinujte:

   ```
   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. Přezkoumejte 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

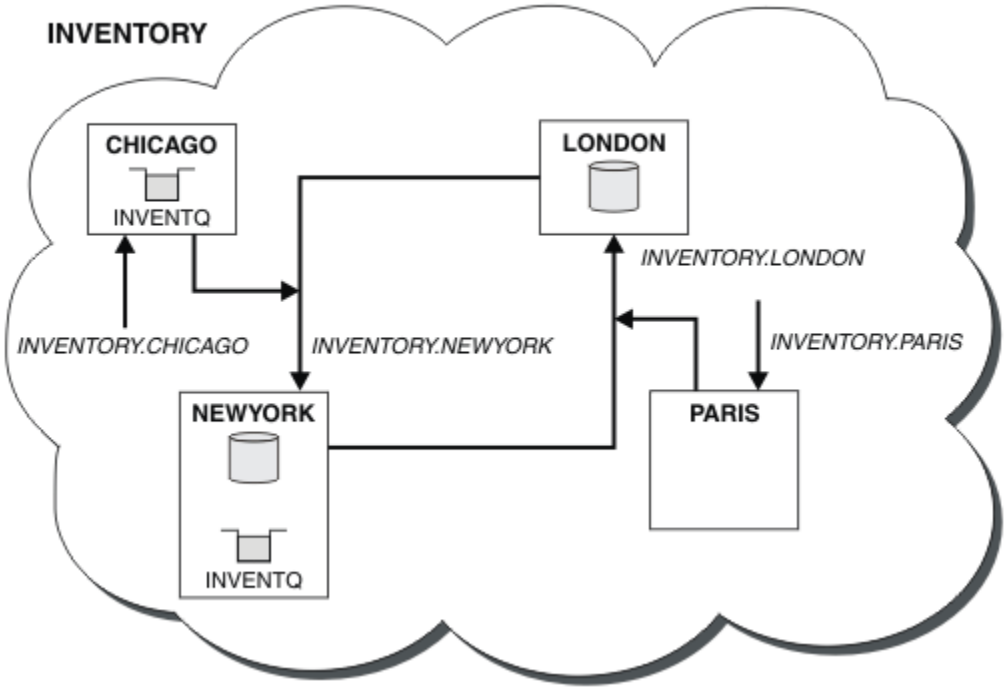
   Server INVENTQ , který je již hostován správcem front NEWYORK , je také hostován jako záloha pomocí CHICAGO. Definujte jej ve správci front produktu CHICAGO takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) CLWLPRTY(1)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte iniciátor kanálu na produktu WebSphere MQ pro z/OS. Na všech platformách spusťte program modulu listener na správci front CHICAGO. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 52 na stránce 263 zobrazuje klastr nastavený touto úlohou.



Obrázek 52. Klastr INVENTORY se čtyřmi správci front

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správcích front v klastru. Správce front produktu CHICAGO je zálohou. Zprávy odeslané do INVENTQ jsou směrovány 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 klastru. 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.

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)
   CONNAME(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)
   CONNAME(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:

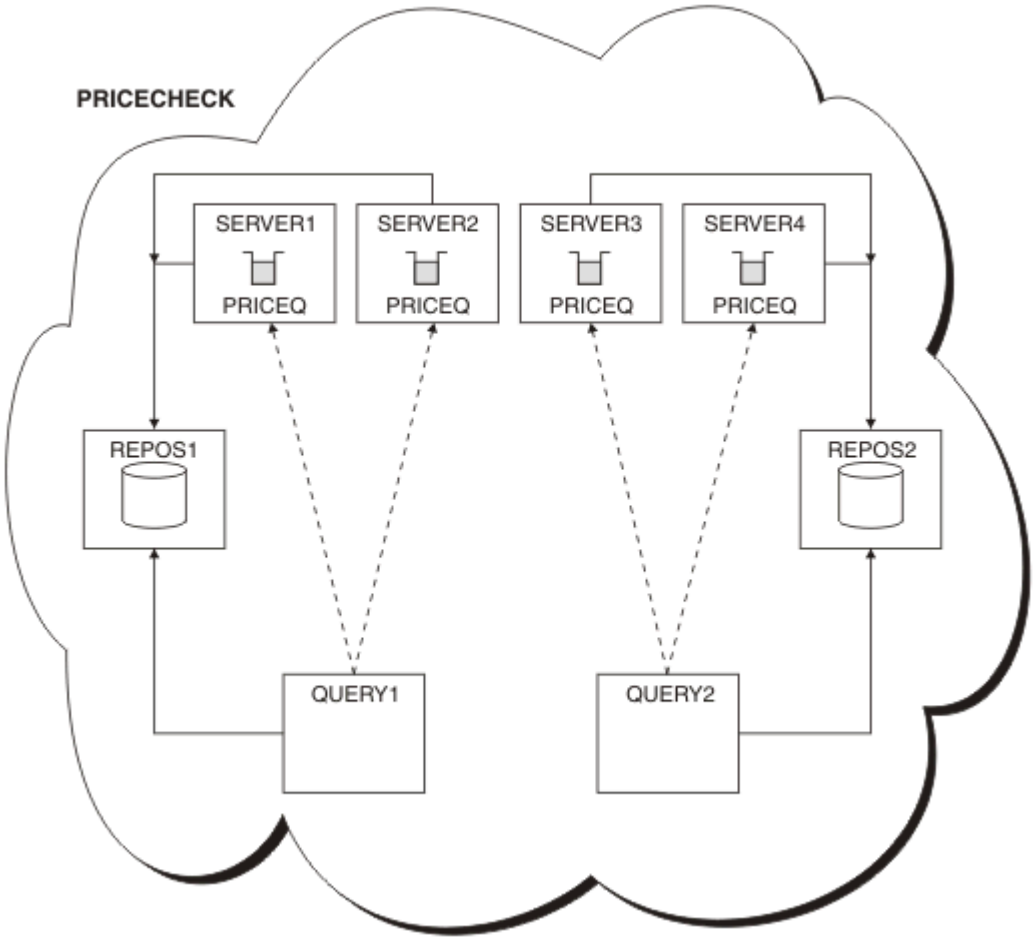
   ```
   ALTER QMGR CLWLMRUC(2)
   ```

7. Pokud jste tak dosud neučinili, spusťte iniciátor kanálu v produktu WebSphere MQ pro 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 53 na stránce 265 zobrazuje klastr nastavený touto úlohou.



Obrázek 53. 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.

Jak pokračovat dále

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.

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:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 191. Obsahuje tři správce front: LONDON a NEWYORK udržují úplná úložiště, PARIS ukládá dílčí úložiště a umisťuje 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)
   CONNAME(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)
   CONNAME(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.

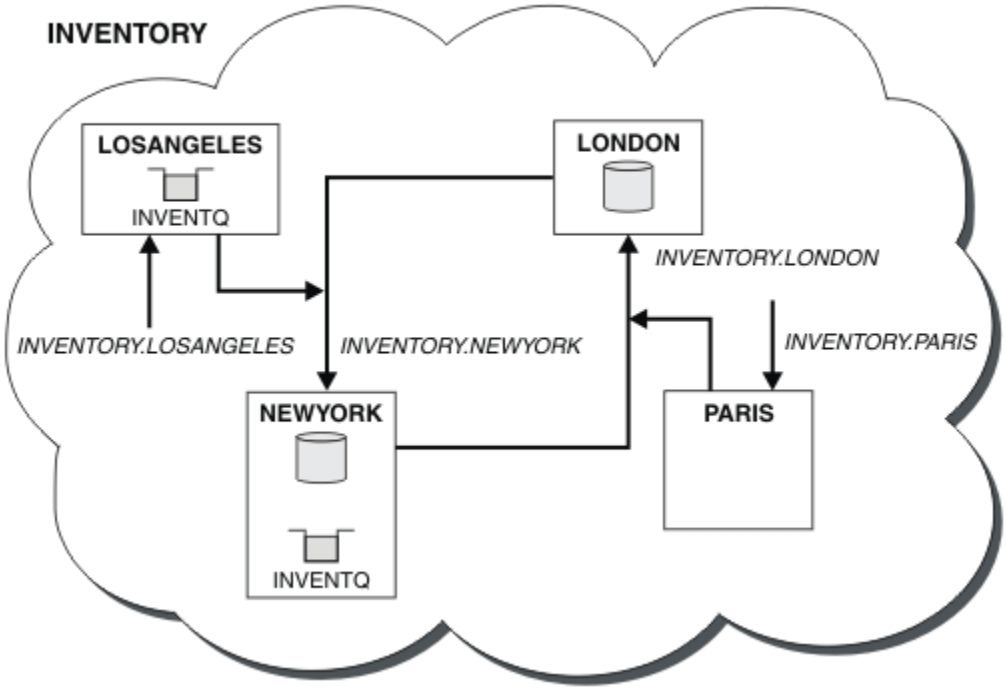
   Frontu INVENTQ , která je již hostována správcem front NEWYORK , je také hostována pomocí LOSANGELES. Definujte jej ve správci front produktu LOSANGELES takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte iniciátor kanálu na produktu WebSphere MQ pro z/OS. Na všech platformách spusťte program modulu listener na správci front LOSANGELES. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

“Přidání výkonnějšího správce front, který je hostitelem fronty” na stránce 265 zobrazuje klastr nastavený touto úlohou.



Obrázek 54. Klastr INVENTORY se čtyřmi správci front

Tato úprava klastru byla dokončena, aniž byste museli měnit správce front LONDON a PARIS. Úložiště v těchto správcích 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 správcích front v klastru. 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 lokálním správci front, kdykoli je to možné. Zprávy zařazené do LONDON nebo PARIS jsou směrovány na LOSANGELES nebo NEWYORK, dvakrát tolik zpráv, které se posílají na LOSANGELES.

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)`.

Práce s afinitními zprávami

Afinity zpráv jsou zřídka součástí dobrého návrhu programování. Chcete-li plně využívat klastrování, je třeba odstranit afinity zprávy. 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:

- Žádající 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 `MQOO_BIND_ON_OPEN` u volání `MQOPEN` .

Vynuťte, aby všechny vaše zprávy byly vloženy do stejného cíle pomocí volby `MQOO_BIND_ON_OPEN` na volání `MQOPEN` . Musí být zadán buď `MQOO_BIND_ON_OPEN` nebo `MQOO_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 `MQOO_BIND_ON_OPEN`se vynutí odeslání všech zpráv, které jsou odeslány do této fronty do stejné instance fronty. `MQOO_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 `MQOO_BIND_ON_OPEN` vynuťte, 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.

`MQOO_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 `MQOO_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 `MQOO_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 `MQOO_BIND_AS_Q_DEF`.

Nastavte volbu `MQOO_BIND_ON_GROUP` u volání `MQOPEN` .

Vynuťte, aby všechny zprávy ve skupině byly vloženy do stejného cíle pomocí volby `MQOO_BIND_ON_GROUP` na volání `MQOPEN` . Musí být zadán buď `MQOO_BIND_ON_OPEN` nebo `MQOO_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 `MQOO_BIND_ON_GROUP`se vynutí odeslání všech zpráv ve skupině, které jsou odeslány do této fronty, do stejné instance fronty. `MQOO_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 `MQOO_BIND_ON_GROUP` vynuťte, 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.

MQOO_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 MQOO_BIND_ON_GROUP, je při otevření fronty vybrána přenosová cesta.

Aby byl produkt MQOO_BIND_ON_GROUP efektivní, musíte zahrnout volbu vložení MQPMO_LOGICAL_ORDER do MQPUT. Můžete nastavit **GroupId** v MQMD zprávy na MQGI_NONEa 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 MQOO_BIND_ON_GROUP , ale zprávy nejsou seskupeny, chování je ekvivalentní hodnotě MQOO_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 MQOO_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 MQOO_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 přesměroval všechny související zprávy do stejného správce front.

Klastrování: doporučené postupy

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

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

Související pojmy
Klastrování
Koncepce interkomunikace
Jak klastry fungují

Klastrování: Speciální pokyny pro překrývající se klastry

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

Vlastnictví klastru

Seznamte se se překrývajícími se klastry před čtením následujících informací. Potřebné informace naleznete v tématech “Překrývání klastrů” na stránce 176 a “Konfigurace cest zpráv mezi klastry” na stránce 251 .

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

- Ačkoli jsou klastry produktu IBM WebSphere MQ 'volně spojené', jak již bylo popsáno dříve, je užitečné považovat klastr jako jedinou jednotku administrace. Tento koncept se používá, protože interakce mezi definicemi na jednotlivých správcích front je kritická pro hladké fungování klastru. Příklad: Při použití front klastru s vyrovnáváním pracovní zátěže je důležité, aby jeden administrátor nebo tým pochopil

úplnou sadu možných cílů pro zprávy, které závisí na definicích rozloženém v rámci klastru. Více triviálně musí být dvojice odesilatel/příjemce klastru kompatibilní v celém rozsahu.

- S ohledem na tento předchozí koncept; pokud se schází více klastrů (které mají být spravovány samostatnými týmy/jednotlivci), je důležité mít jasné zásady v místě řízení administrace správců front brány.
- Je užitečné zacházet s překrývajícími se klastry jako s jedním oborem názvů: Názvy kanálů a názvy správců front musí být jedinečné v rámci jediného klastru. Administrace je mnohem jednodušší, když je v celé topologii jedinečná. Nejlepší je následovat vhodnou konvenci pojmenování, možné konvence jsou popsány v “Konvence pojmenování klastrů” na stránce 175.
- Někdy je nezbytná spolupráce správy a správy systému: Například spolupráce mezi organizacemi, které vlastní různé klastry a které se musí překrývat. Jasné porozumění toho, kdo vlastní, a vynutitelné pravidla/konvence pomáhá klastrování při překrývání klastrů.

Překrývání klastrů: Komunikační brány

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

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

- Pokud máte soustředné klastry, kde je menší, pro publikování/odběr. Další informace naleznete v tématu Jak změnit velikost systémů .
- Mají-li být někteří správci front spravovány různými týmy. Další informace naleznete v předchozí části “Vlastnictví klastru” na stránce 270.
- Pokud má smysl z organizačního nebo geografického hlediska.
- Pokud ekvivalentní klastry pracují s rozlišováním názvů, například při implementaci zabezpečení SSL nebo TLS v existujícím klastru.

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

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

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

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

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

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

Související pojmy

“Konvence pojmenování klastrů” na stránce 175

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

Klastrování: Aspekty návrhu topologie

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

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

Výkon klastrové infrastruktury

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

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

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

Úplná úložiště

Úložiště je kolekce informací o správcích front, kteří jsou členy klastru. Správce front, který je hostitelem úplné sady informací o každém správci front v klastru, má úplné úložiště. Další informace o úplných úložištích a o částečných úložištích najdete v tématu "Úložiště klastru" na stránce 160.

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

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

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

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

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

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

Měly by aplikace používat fronty v úplných úložištích?

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

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

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

Správa definic kanálů

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

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

Je-li správce front členem více klastrů, existuje volba pro použití jediné definice kanálu se seznamem názvů klastru, nikoli k definování samostatného kanálu produktu CLUSRCVR pro každý klastr. Toto nastavení však může způsobit potíže administrace později; zvažte například případ, kdy má být zabezpečení SSL použito na jeden klastr, nikoli však na sekundu. Proto je vhodné vytvořit oddělené definice a konvence pojmenování navržené v produktu “Konvence pojmenování klastrů” na stránce 175 to podporují.

Vyrovnávání zátěže pomocí více kanálů

Tyto informace jsou určeny jako rozšířené porozumění subjektu. Základní vysvětlení tohoto tématu (které musí být pochopeno před použitím těchto informací) viz “Použití klastrů pro správu pracovní zátěže” na stránce 255, Vyrovnávání pracovní zátěže a Algoritmus správy pracovní zátěže klastru.

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

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

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

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

Klastrování: izolace aplikace pomocí více přenosových front klastru

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

Když implementujete aplikaci, máte na výběr, které prostředky produktu IBM WebSphere MQ sdílí s ostatními aplikacemi a které prostředky se o ní nesdílí. Existuje celá řada typů prostředků, které lze sdílet, přičemž hlavní jsou servery samotné, správce front, kanály a fronty. Můžete zvolit konfiguraci aplikací s menším počtem sdílených prostředků; alokací samostatných front, kanálů, správců front nebo dokonce serverů pro jednotlivé aplikace. Pokud tak učiníte, bude celková konfigurace systému mnohem větší a složitější. Použití klastru IBM WebSphere MQ snižuje složitost správy více serverů, správců front, front a kanálů, ale zavádí další sdílený prostředek, přenosovou frontu klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Obrázek 55 na stránce 276 je výseč velké implementace produktu IBM WebSphere MQ , která ilustruje významnost sdílení `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. V diagramu je aplikace, `Client App`, připojena ke správci front `QM2` v klastru `CL1`. Zpráva od `Client App` je zpracována aplikací, `Server App`. Zpráva je načtena příkazem `Server App` z fronty klastru `Q1` ve správci front `QM3` v `CLUSTER2`. Vzhledem k tomu, že klientské a serverové aplikace nejsou ve stejném klastru, je zpráva přenesena správcem front brány `QM1`.

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

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

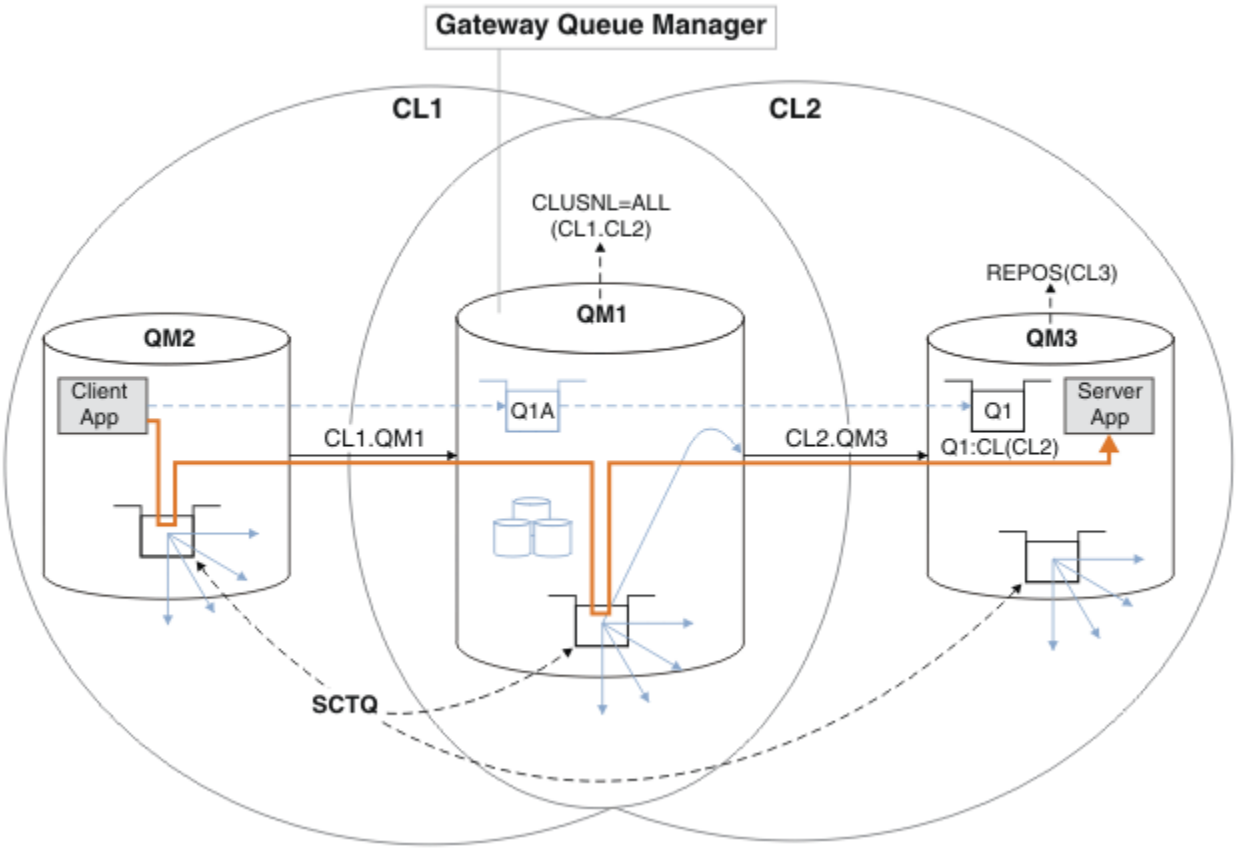
Z hlediska výkonu se nejedná o problém s jedinou frontou. Společná přenosová fronta obecně nereprezentuje kritické místo výkonu. Propustnost zpráv na bráně je do značné míry určena výkonem kanálů, které se k ní připojují. Propustnost není obecně ovlivněna počtem front, nebo počtem zpráv ve frontách,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

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

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

  Pokud se jeden cíl klastru stane nedostupným, zprávy pro toto místo určení se zobrazí v jedné přenosové frontě a zprávy se nakonec zaplní. Jakmile je přenosová fronta plná, zastaví vkládání zpráv do přenosové fronty pro jakékoli místo určení klastru.

- Přenos zpráv do různých cílů klastru není snadný. Všechny zprávy jsou na jedné přenosové frontě. Zobrazení hloubky přenosové fronty vám dává málo informací o tom, zda jsou zprávy přenášeny do všech míst určení.



Poznámka: Šipky v Obrázek 55 na stránce 276 a následující čísla jsou různého typu. Pevné šipky představují toky zpráv. Popisky na pevných šipkách jsou názvy kanálů zpráv. Šedé pevné šipky představují potenciální toky zpráv z `SYSTEM.CLUSTER.TRANSMIT.QUEUE` do kanálů odesílatele klastru. Černá přerušovaná čára spojuje popisky s jejich cíli. Šedé šířené šipky jsou odkazy; například z volání `MQOPEN` z `Client App` do definice fronty aliasu klastru `Q1A`.

Obrázek 55. Aplikace Client-server implementovaná do rozbočovače a mluvila s architekturou pomocí klastrů produktu IBM WebSphere MQ .

V produktu Obrázek 55 na stránce 276jsou klienti produktu `Server App` otevření fronty `Q1A`. Zprávy se umístí do `SYSTEM.CLUSTER.TRANSMIT.QUEUE` na `QM2`, přenesou se do `SYSTEM.CLUSTER.TRANSMIT.QUEUE` na `QM1`a pak jsou přeneseny do `Q1` na `QM3`, kde jsou přijímány aplikací `Server App` .

Zpráva z produktu `Client App` prochází přes přenosové fronty klastru systému v systémech `QM2` a `QM1`. V produktu Obrázek 55 na stránce 276je cílem izolovat tok zpráv od správce front brány od klientské aplikace, aby jeho zprávy nebyly uloženy v systému `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Toky můžete izolovat od všech ostatních klastrovaných správců front. Můžete také izolovat toky v opačném směru, zpět ke klientovi. Chcete-li uchovat popis řešení stručný, popisy považují pouze jeden tok z aplikace klienta.

Řešení pro izolaci provozu zpráv klastru ve správci front brány klastru

Jednou z možností k vyřešení problému je použití aliasů správce front nebo definic vzdálených front k přemostění mezi klastry. Vytvořte klastrované vzdálené definice fronty, přenosové fronty a kanál, které oddělují jednotlivé toky zpráv ve správci front brány, viz “Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195.

Od produktu Version 7.5 se správci front klastru neomezují pouze na jednu přenosovou frontu klastru. Můžete vybrat ze dvou voleb:

1. Definujte další přenosové fronty klastru ručně a definujte, které odesílací kanály klastru budou přenášet zprávy z jednotlivých přenosových front; viz “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198.
2. Umožněte správci front automaticky vytvářet a spravovat další přenosové fronty klastru. Definuje jinou přenosovou frontu klastru pro každý odesílací kanál klastru; viz “Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv” na stránce 217

Můžete sloučit ručně definované přenosové fronty klastru pro některé odesílací kanály klastru, přičemž správce front spravuje zbytek. Kombinace přenosových front je přístup, který se používá v produktu “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198. V tomto řešení se většina zpráv mezi klastry používá běžnou `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Jedna aplikace je kritická a všechny její toky zpráv jsou izolovány od ostatních toků pomocí jedné ručně definované přenosové fronty klastru.

Konfigurace v produktu “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 198je omezena. Neoddělují provoz zpráv do fronty klastru ve stejném klastru ve stejném klastru jako jiná fronta klastru. Přenos zpráv do jednotlivých front můžete oddělit pomocí definic vzdálených front, které jsou součástí distribuovaných front. U klastrů, které používají více přenosových front klastru, můžete oddělit provoz zpráv, který bude směřovat do různých odesílacích kanálů klastru. Více front klastru ve stejném klastru, ve stejném správci front, sdílejí odesílací kanál klastru. Zprávy pro tyto fronty jsou uloženy ve stejné přenosové frontě před tím, než jsou přeposlána ze správce front brány. V konfiguraci v produktu “Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 201je omezení tímto způsobem omezeno přidáním dalšího klastru a vytvořením správce front a klastrové fronty členem nového klastru. Nový správce front může být jediným správcem front v klastru. Do klastru můžete přidat více správců front a pomocí stejného klastru izolovat fronty klastru také u těchto správců front.

Související pojmy

“Řízení přístupu a více přenosových front klastru” na stránce 157
Zvolte mezi třemi režimy kontroly, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na `SYSTEM.CLUSTER.TRANSMIT.QUEUE`, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

“Klastrování: Speciální pokyny pro překrývající se klastry” na stránce 270
Toto téma obsahuje pokyny pro plánování a administraci klastrů IBM WebSphere MQ . Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

“Přenosové fronty klastru a odesílací kanály klastru” na stránce 167
Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru.

“Překrývání klastrů” na stránce 176
Překrývající se klastry poskytují další administrativní schopnosti. Použijte seznamy názvů ke snížení počtu příkazů potřebných pro správu překrývajících se klastrů.

Související úlohy

Autorizace vkládání zpráv ve vzdálených frontách klastru

“Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195
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” na stránce 198
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 201
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” na stránce 217
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.

“Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

“Konfigurace cest zpráv mezi klastry” na stránce 251
Připojte klastry pomocí správce front brány. Zviditelněte fronty nebo správce front pro všechny klastry definováním aliasů front klastru nebo správců front klastru ve správci front brány.

“Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278
Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

Související odkazy
“Zabezpečení” na stránce 418
Použijte sekci `Security` v souboru `qm.ini` , abyste uvedli volby pro OAM (Object Authority Manager).

setmqaut

Klastrování: Plánování konfigurace přenosových front klastru

Jste provedeni pomocí voleb přenosových front klastru. Můžete nakonfigurovat jednu běžnou výchozí frontu, oddělenou výchozí frontu nebo ručně definované fronty. Konfigurace více přenosových front klastru platí pro platformy jiné než z/OS.

Než začnete

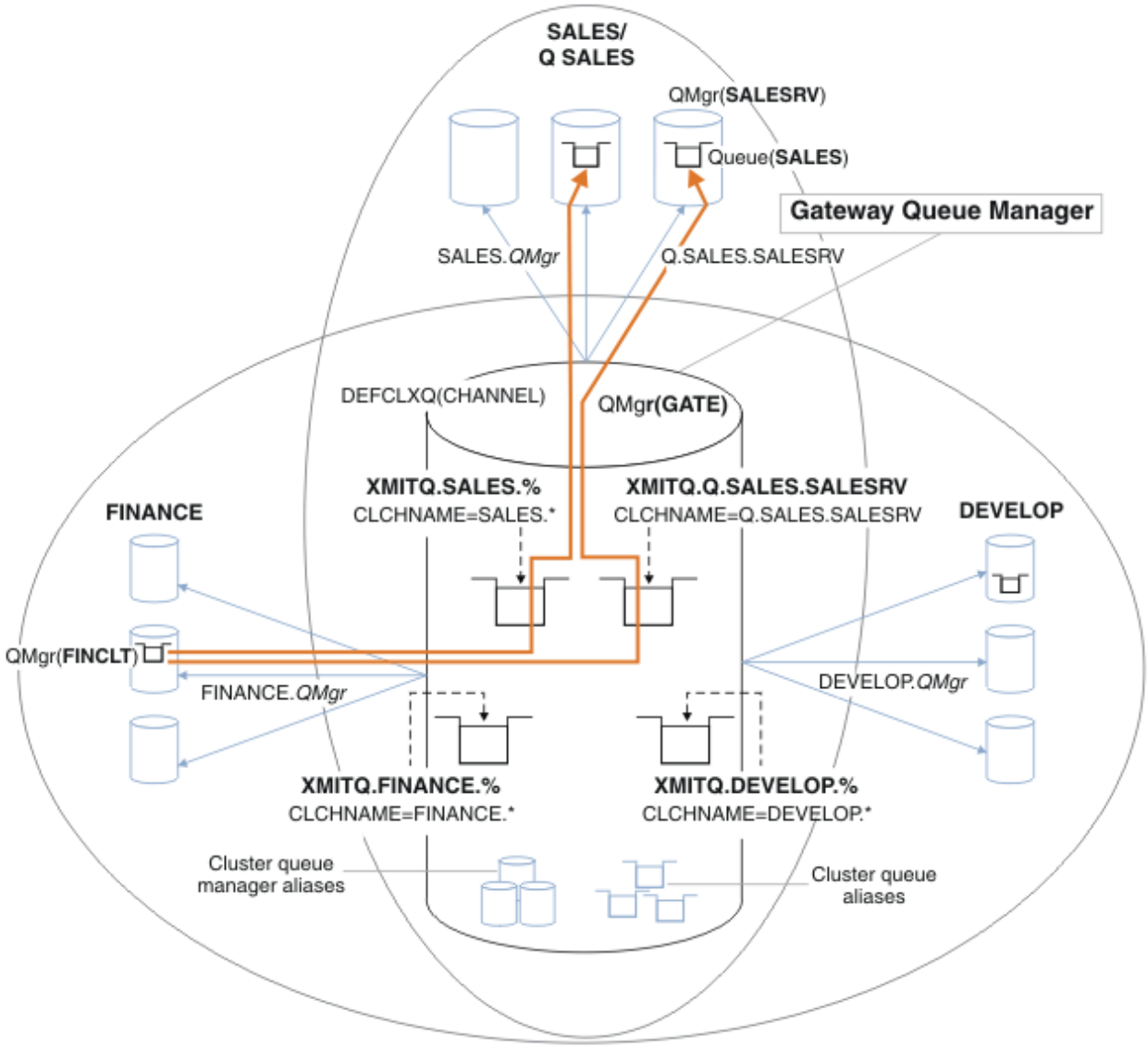
Zkontrolujte “Jak se rozhodnout, jaký typ přenosové fronty klastru použít” na stránce 281.

Informace o této úloze

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

1. Jaká je výchozí přenosová fronta klastru pro přenosy zpráv klastru?
   a. Společná přenosová fronta klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.
   b. Oddělit přenosové fronty klastru. Správce front spravuje oddělené přenosové fronty klastru. Vytvoří je jako trvalé-dynamické fronty z modelové fronty, `SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE`. Vytvoří jednu přenosovou frontu klastru pro každý odesílací kanál klastru, který používá.
2. Pro přenosové fronty klastru, které se rozhodnete vytvořit ručně, máte další dvě možnosti:
   a. Definujte samostatnou přenosovou frontu pro každý odesílací kanál klastru, který se rozhodnete nakonfigurovat ručně. V tomto případě nastavte atribut fronty **CLCHNAME** přenosové fronty na název kanálu odesílatele klastru. Vyberte odesílací kanál klastru, který má přenášet zprávy z této přenosové fronty.
   b. Kombinujte provoz zpráv pro skupinu odesílacích kanálů klastru do stejné přenosové fronty klastru, viz Obrázek 56 na stránce 279. V tomto případě nastavte atribut fronty **CLCHNAME** každé společné přenosové fronty na generický název kanálu odesílatele klastru. Generický název kanálu odesílatele klastru je filtr pro seskupení názvů odesílacích kanálů klastru. Například skupina

SALES.* seskupuje všechny kanály odesílatele klastru, jejichž názvy začínají řetězcem SALES.. Do řetězce filtru můžete umístit více zástupných znaků. Zástupný znak je hvězdička, "*". Představuje od nuly po libovolný počet znaků.



Obrázek 56. Příklad specifických přenosových front pro různé klastry oddělení IBM WebSphere MQ

Postup

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

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

   ```
   ALTER QMGR DEFCLXQ(CHANNEL)
   ```
2. Izolovat jakékoli toky zpráv, které nesmí sdílet přenosovou frontu klastru s jinými toky.
   - Viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 283. V příkladu je to fronta SALES , která musí být izolována, je členem klastru SALES , na SALESRV. Chcete-li izolovat frontu SALES , vytvořte nový klastr Q.SALES, vytvořte člena SALESRV správce front a upravte frontu SALES tak, aby patřila do produktu Q.SALES.

- Správci front, kteří odesílají zprávy do produktu SALES , musí být zároveň členy nového klastru. Pokud používáte alias klastrované fronty a správce front brány jako v příkladu, můžete v mnoha případech omezit změny, aby správce front brány mohl být členem nového klastru.
- Oddělením toků od brány k cíli však do brány ze zdrojového správce front neoddělují toky. Ale občas se ukáže, že stačí k oddělení toků od brány a ne toku do brány. Pokud to není dostatečné, přidejte do nového klastru zdrojového správce front. Pokud chcete, aby zprávy cestovali přes bránu, přesuňte alias klastru do nového klastru a pokračujte v odesílání zpráv na alias klastru na bráně a nikoli přímo do cílového správce front.

Chcete-li izolovat toky zpráv, postupujte takto:

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

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

- Viz “Klastrování: Speciální pokyny pro překrývající se klastry” na stránce 270.

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

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

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

- Typické řízení a požadavky na monitorování mají za následek přenosovou frontu na klastr nebo přenosovou frontu na správce front. Pokud postupujete podle konvence pojmenování pro kanály klastru, *`ClusterName.QueueManagerName`*, je snadné vytvořit generické názvy kanálů, které vyberou klastr správců front nebo všechny klastry, jejichž členem je správce front; viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 283.
- Rozšiřte konvence pojmenování pro přenosové fronty klastru tak, aby vyhovdily generickým názvům kanálů, nahrazením symbolu hvězdičky znakem procent. Například

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

Související pojmy

“Přenosové fronty klastru a odesílací kanály klastru” na stránce 167
Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru.

“Klastrování: izolace aplikace pomocí více přenosových front klastru” na stránce 275
Můžete izolovat toky zpráv mezi správci front v klastru. Zprávy přenášená různými kanály odesílatele klastru můžete umisťovat do různých přenosových front klastru. Přístup můžete použít v jednom klastru nebo s překrývajícími se klastry. Toto téma obsahuje příklady a některé osvědčené postupy, které vás provedou při výběru přístupu k použití.

“Řízení přístupu a více přenosových front klastru” na stránce 157
Zvolte mezi třemi režimy kontroly, kdy aplikace vkládá zprávy do vzdálených front klastru. Režimy se kontrolují vzdáleně vůči frontě klastru, kontrolují lokálně na `SYSTEM.CLUSTER.TRANSMIT.QUEUE`, nebo kontrolují lokální profily pro frontu klastru nebo správce front klastru.

“Klastrování: Speciální pokyny pro překrývající se klastry” na stránce 270
Toto téma obsahuje pokyny pro plánování a administraci klastrů IBM WebSphere MQ . Tyto informace jsou pokyny založené na testování a zpětné vazbě od zákazníků.

“Překrývání klastrů” na stránce 176
Překrývající se klastry poskytují další administrativní schopnosti. Použijte seznamy názvů ke snížení počtu příkazů potřebných pro správu překrývajících se klastrů.

Související úlohy

“Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 195
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" na stránce 198
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 201
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" na stránce 217
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.

"Vytvoření dvou překrývajících se klastrů se správcem front brány" na stránce 212
Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv pro jednu aplikaci ze zpráv pro jiné aplikace v klastru.

"Konfigurace cest zpráv mezi klastry" na stránce 251
Připojte klastry pomocí správce front brány. Zviditelněte fronty nebo správce front pro všechny klastry definováním aliasů front klastru nebo správců front klastru ve správci front brány.

Jak se rozhodnout, jaký typ přenosové fronty klastru použít

Jak si vybrat mezi různými volbami konfigurace přenosové fronty klastru.

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

1. Můžete mít všechny odesílací kanály klastru přidružené k jedné výchozí přenosové frontě klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Tato volba je výchozí a je jediná volba pro správce front, kteří pracují s verzí Version 7.1nebo starší.
2. Všechny odesílací kanály klastru můžete nastavit tak, aby byly automaticky přidruženy k samostatné přenosové frontě klastru. Fronty jsou vytvořeny správcem front z modelové fronty `SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE` s názvem `SYSTEM.CLUSTER.TRANSMIT.`*`ChannelName`*. Kanály budou používat vysílací frontu s jedinečným názvem v případě, že je atribut správce front **DEFCLXQ** nastaven na hodnotu `CHANNEL`.

   Upozornění: Používáte-li vyhrazené `SYSTEM.CLUSTER.TRANSMIT.QUEUES` se správcem front, který byl upgradován z dřívější verze produktu, ujistěte se, že `SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE` má volbu SHARE/NOSHARE nastavenou na **SHARE**.
3. Můžete nastavit konkrétní odesílací kanály klastru, které mají být obsluhovány jednou přenosovou frontou klastru. Vyberte tuto volbu tak, že vytvoříte přenosovou frontu a nastavíte její atribut **CLCHNAME** na název kanálu odesílatele klastru.
4. Můžete vybrat skupiny odesílacích kanálů klastru, které mají být obsluhovány jednou přenosovou frontou klastru. Vyberte tuto volbu tak, že vytvoříte přenosovou frontu a nastavíte její atribut **CLCHNAME** na generický název kanálu, jako například *`ClusterName`*`.*`. Pokud pojmenujete kanály klastru podle následujících konvencí pojmenování v produktu "Klastrování: Speciální pokyny pro překrývající se klastry" na stránce 270, tento název vybere všechny kanály klastru připojené ke správcům front v klastru *`ClusterName`*.

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

Doporučené postupy

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

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

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

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

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

Pokud jsou zprávy směrovány přes centrální správce front, jako je například přenosová brána klastru, sdílejí společnou přenosovou frontu SYSTEM.CLUSTER.TRANSMIT.QUEUE. Pokud počet zpráv uložených ve správci front v produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE ve správci front brány dosáhne své maximální hloubky, správce front začne odmítat nové zprávy pro přenosovou frontu, dokud nedojde ke snížení její hloubky. Přetížení ovlivňuje zprávy pro všechna místa určení, která jsou směrována přes bránu. Zprávy zálohují přenosové fronty ostatních správců front, kteří odesílají zprávy do komunikační brány. Problém se projevuje ve zprávách zapisovaných do protokolů chyb správce front, klesající propustnosti zpráv a uplynulé doby mezi odesláním zprávy a časem, kdy zpráva dorazí do místa určení.

Vliv přetížení na jednotlivé přenosové fronty může být zřejmý, i před tím, než je plný. Pokud máte smíšený přenos zpráv a některé velké přechodné zprávy a některé malé zprávy, doba pro doručení malých zpráv se zvýší, když se zaplní přenosová fronta. Zpoždění je způsobeno zápisem velkých přechodných zpráv na disk, které by normálně nebyly zapsány na disk. Pokud máte kritické toky zpráv, sdílíte přenosovou frontu klastru s jinými smíšenými toky se smíšenými zprávami, může být vhodné nakonfigurovat speciální cestu zprávy a izolovat ji od jiných toků zpráv; viz “Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 201

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

Změňte atribut správce front **DEFCLXQ** , který řídí výchozí přenosovou frontu klastru, chcete-li vytvořit různé přenosové fronty klastru pro každý odesílací kanál klastru. Více míst určení může sdílet kanál odesílatele klastru, takže musíte naplánovat úplné splnění tohoto cíle v klastrech. Systematicky použijte metodu “Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 201 na všechny fronty klastru. Výsledkem, jehož cílem je, aby se nesdílely kanál odesílatele klastru s jiným místem určení klastru, není cílem žádného cíle klastru. V důsledku toho žádná zpráva pro místo určení klastru sdílí svou přenosovou frontu klastru se zprávou jiného místa určení.

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

Související úlohy

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

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

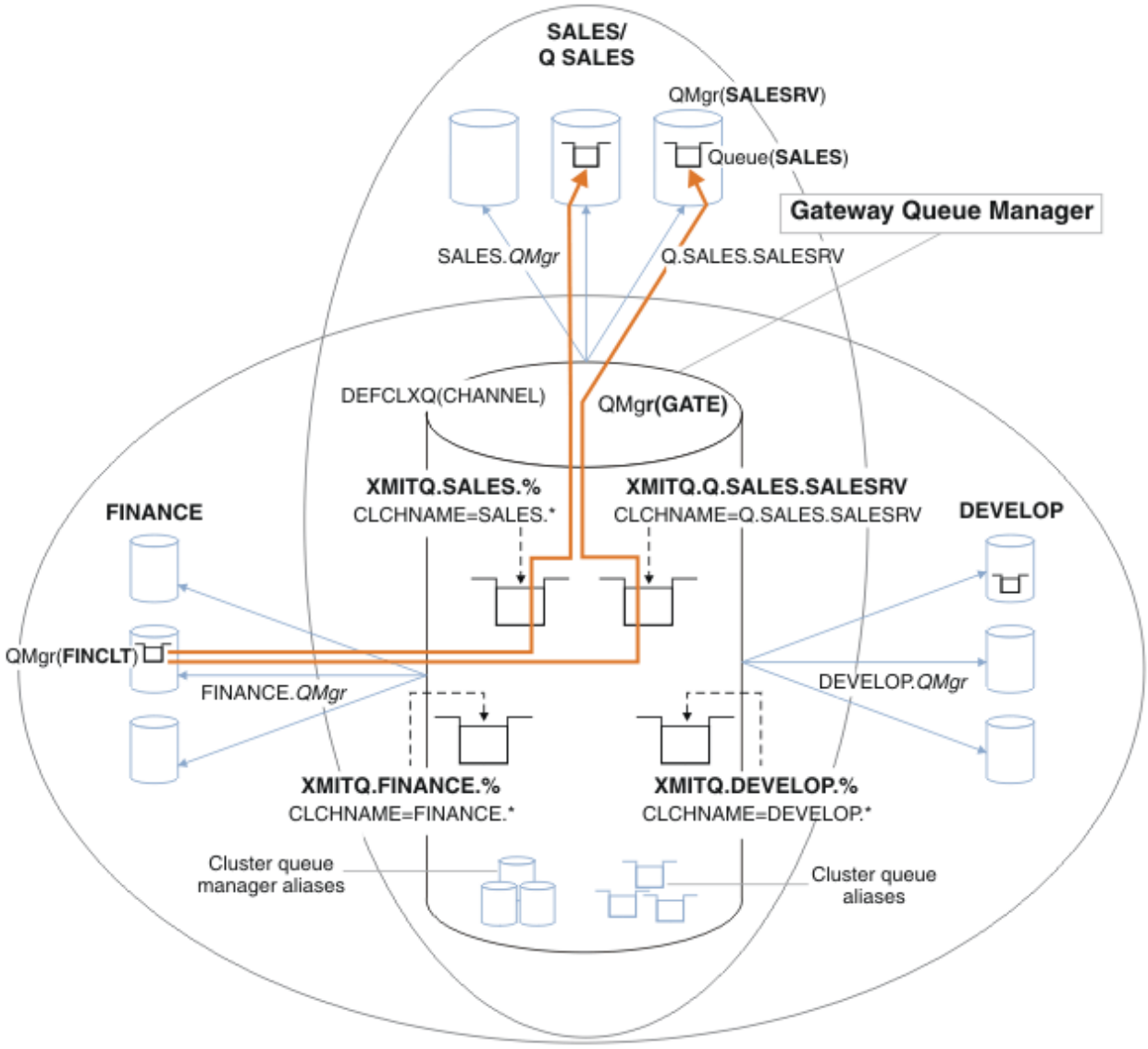
Klastrování: Příklad konfigurace více přenosových front klastru

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

Informace o této úloze

Kroky v této úloze ukazují, jak použít proceduru v produktu “Klastrování: Plánování konfigurace přenosových front klastru” na stránce 278 a dospět k konfiguraci zobrazené v Obrázek 57 na stránce 284. Jedná se o příklad tří překrývajících se klastrů, se správcem front brány, který je konfigurován s oddělenými frontami přenosu klastru. Příkazy MQSC pro definování klastrů jsou popsány v tématu “Vytváření ukázkových klastrů” na stránce 286.

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



Obrázek 57. Příklad specifických přenosových front pro různé klastry oddělení IBM WebSphere MQ

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

Postup

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

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

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

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

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

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

Tento příklad vyžaduje přidání správce front SALESRV do nového klastru v rámci prodejního oddělení. Máte-li několik front, které vyžadují izolaci, můžete se rozhodnout pro vytvoření specifického klastru pro frontu SALES . Možnou konvencí pojmenování pro název klastru je pojmenování takových klastrů, `Q.` *QueueName*, například `Q.SALES` . Alternativním přístupem, který může být praktičtější, pokud máte velký počet front, které mají být izolovány, je vytvořit klastry izolovaných front tam a kde je to potřeba. Názvy klastrů mohou být `QUEUES.`*n*.

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

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

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

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

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

Fronta SALES je členem obou klastrů, právě pro přechod. Jakmile je nová konfigurace spuštěna, odeberte frontu produktu SALES z klastru SALES , viz Obrázek 58 na stránce 289.

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

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

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

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

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

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

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

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

3. Třetí konfigurační krok je k " Vytvořte přenosové fronty klastru, které budou odpovídat požadavkům řízení nebo monitorování".

Ve správci front brány definujte přenosové fronty klastru:

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

Jak pokračovat dále

Přepněte na novou konfiguraci ve správci front brány.

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

1. Zastavte následující kanály ve správci front brány:

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

2. Spusťte následující kanály ve správci front brány:

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

Jakmile je přepínač dokončen, odeberte frontu produktu SALES z klastru SALES , viz Obrázek 58 na stránce 289.

Související pojmy

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

Související úlohy

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

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

Informace o této úloze

Úplné příkazy produktu **MQSC** pro vytvoření klastrů FINANCE, SALESa Q.SALES jsou poskytovány v části Definice pro základní klastry, Změny k izolaci prodejní fronty v novém klastru a oddělené přenosové fronty klastru bránya Odeberte prodejní frontu ve správci front SALESRV z klastru prodeje. Klastr DEVELOP je vynechán z definic, aby byly definice kratší.

Postup

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

      Spusťte příkaz: `crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE` *QmgrName* pro každý z názvů správce front v produktu Tabulka 27 na stránce 286.

Tabulka 27. Názvy a čísla portů správce front

Popis	Název správce front	Číslo portu
Finanční úložiště	FINR1	1414
Finanční úložiště	FINR2	1415
Finanční klient	FINCLT	1418
Prodejní úložiště	SALER1	1416
Prodejní úložiště	SALER2	1417
Prodejní server	SALESRV	1419
Komunikační brána	GATE	1420

b) Spustit všechny správce front

Spusťte příkaz: `strmqm` *QmgrName* pro každý z názvů správce front v produktu Tabulka 27 na stránce 286.

c) Vytvořte definice pro každého správce front.

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

Definice pro základní klastry

finr1.txt

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

finr2.txt

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

finclt.txt

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

saler1.txt

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

saler2.txt

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

salesrv.txt

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

gate.txt

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

2. Otestujte konfiguraci spuštěním ukázkového programu požadavku.
   a) Spuštění programu pro monitorování spouštěčů ve správci front produktu SALESRV

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

   b) Spusťte vzorový program požadavku a odešlete požadavek.

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

      Zpráva požadavku se ozývá zpět a po 15 sekundách, kdy ukázkový program skončí.
3. Vytvořte definice, abyste izolovali frontu SALES v klastru `Q.SALES` a oddělili zprávy klastru pro klastr SALES a FINANCE ve správci front brány.

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

   Změny k izolování prodejní fronty v novém klastru a oddělené přenosové fronty klastru brány
   chgsaler1.txt

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

   chgsaler2.txt

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

   chgsalesrv.txt

```
DEFINE NAMELIST (CLUSTERS) NAMES(SALES, Q.SALES)
DEFINE CHANNEL(Q.SALES.SALER1)  CHLTYPE(CLUSSDR)  CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.SAVESRV) CHLTYPE(CLUSRCVR) CONNAME('localhost(1419)')
CLUSTER(Q.SALES) REPLACE
ALTER  QLOCAL (SALES) CLUSTER(' ') CLUSNL(CLUSTERS)
```

   chggate.txt

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

4. Odeberte frontu SALES z klastru SALES .

   Spusťte příkaz **MQSC** v systému Obrázek 58 na stránce 289:

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

   Obrázek 58. Odebrat prodejní frontu ve správci front SALESRV z klastru prodeje
5. Přepněte kanály na nové přenosové fronty.

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

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

Jak pokračovat dále

1. Znovu spusťte ukázkový program požadavku a ověřte, že nová konfigurace funguje; viz krok “2” na stránce 288
2. Monitorujte zprávy proudící všemi frontami přenosu klastru ve správci front GATE :
   a. Upravte definici každé přenosové fronty klastru tak, aby se monitorování fronty zapnul.

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

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

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

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

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

   e. Výsledky za několik intervalů jsou následující:

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

```
  GetBytes: [435, 0]
  ...
QueueStatistics: 1
  QueueName: 'SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV'
  CreateDate: '2012-02-24'
  CreateTime: '16.37.43'
  ...
  PutCount: [1, 0]
  PutFailCount: 0
  Put1Count: [0, 0]
  Put1FailCount: 0
  PutBytes: [435, 0]
  GetCount: [1, 0]
  GetBytes: [435, 0]
  ...
MonitoringType: QueueStatistics
QueueManager: 'GATE'
IntervalStartDate: '2012-02-27'
IntervalStartTime: '15.00.20'
IntervalEndDate: '2012-02-27'
IntervalEndTime: '15.01.20'
CommandLevel: 700
ObjectCount: 2
QueueStatistics: 0
  QueueName: 'SYSTEM.CLUSTER.TRANSMIT.QUEUE'
  CreateDate: '2012-02-24'
  CreateTime: '15.58.15'
  ...
  PutCount: [2, 0]
  PutFailCount: 0
  Put1Count: [0, 0]
  Put1FailCount: 0
  PutBytes: [863, 0]
  GetCount: [2, 0]
  GetBytes: [863, 0]
  ...
QueueStatistics: 1
  QueueName: 'SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV'
  CreateDate: '2012-02-24'
  CreateTime: '16.37.43'
  ...
  PutCount: [2, 0]
  PutFailCount: 0
  Put1Count: [0, 0]
  Put1FailCount: 0
  PutBytes: [863, 0]
  GetCount: [2, 0]
  GetBytes: [863, 0]
  ...
2 Records Processed.
```

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

Klastrování: Přepnutí přenosových front klastru

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

Než začnete

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přechod bude rychlejší. Než budete pokračovat dále, přečtěte si “Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje” na stránce 170 , abyste zjistili důvody pro pokus o vyprázdnění přenosové fronty.

Informace o této úloze

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

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

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

Procedura

- Volba 1: Nechat správce front provést změny automaticky; viz “Přepínání aktivních odesílacích kanálů klastru na jinou sadu front-přenosových front” na stránce 292.

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

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

  Vyberete-li tuto volbu tím, že necháte přepínač automaticky, spustí se proces přepínání při spuštění kanálu odesílatele klastru. Není-li kanál zastaven, bude spuštěn poté, co se stane neaktivní, pokud bude existovat nějaká zpráva ke zpracování. Je-li kanál zastaven, spusťte jej pomocí příkazu START CHANNEL .

  Proces přepnutí se dokončí, jakmile v přenosové frontě kanálu, který kanál obsluhuje, nezůstalo žádné zprávy, které byly ponechány pro odesílací kanál klastru. Jakmile je tomu tak, jsou nově příchozí zprávy pro odesílací kanál klastru ukládány přímo do nové přenosové fronty. Do té doby jsou zprávy ukládány do staré přenosové fronty a proces přepínání přenáší zprávy ze staré přenosové fronty do nové přenosové fronty. Odesílací kanál klastru předává zprávy z nové přenosové fronty klastru během celého procesu přepínání.

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

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

- Volba 2: Proveďte změny ručně; viz “Přepnutí zastaveného odesílacího kanálu klastru do jiné přenosové fronty klastru” na stránce 293.

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

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

  Vyberete-li tuto volbu, máte úplnou kontrolu nad tím, kdy dojde k přepnutí.

Můžete si být jisti o dokončení procesu přepínání v pevně stanoveném čase, v rámci okna údržby. Doba, kterou přepnutí zabere, závisí na tom, kolik zpráv se má přenést z jedné přenosové fronty do druhé. Pokud se zprávy dostaví, může chvíli trvat, než bude proces přenášet všechny zprávy.

Máte možnost přepnout kanál bez přenosu zpráv ze staré přenosové fronty. Přepínač je "instant". Když restartujete odesílací kanál klastru, začne zpracovávat zprávy v přenosové frontě, kterou jste k ní nově přiřadili.

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

Související pojmy

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

Související úlohy

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

“Přepínání aktivních odesílacích kanálů klastru na jinou sadu front-přenosových front” na stránce 292
Tato úloha vám poskytuje tři volby pro přepínání aktivních odesílacích kanálů klastru. Jednou z možností je nechat správce front přepnout přepínač automaticky, což nemá vliv na běžící aplikace. Další volby slouží k ručnímu zastavení a spuštění kanálů nebo k restartování správce front.

“Přepnutí zastaveného odesílacího kanálu klastru do jiné přenosové fronty klastru” na stránce 293

Související informace

“Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje” na stránce 170

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

Než začnete

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

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přechod bude rychlejší. Než budete pokračovat dále, přečtěte si “Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje” na stránce 170 , abyste zjistili důvody pro pokus o vyprázdnění přenosové fronty.

Informace o této úloze

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

Postup

1. Volitelné: Zaznamenat aktuální stav kanálu

   Vytvořte záznam o stavu aktuálních a uložených kanálů, které obsluhují přenosové fronty klastru. Následující příkazy zobrazují stav vztahující se k přenosovým frontám systémového klastru. Přidejte své vlastní příkazy, abyste zobrazili stav přidružený k frontám přenosu klastru, které jste definovali.

Použijte konvenci, jako například XMITQ.*ChannelName*, abyste pojmenovali přenosové fronty klastru, které definujete, aby bylo snadné zobrazit stav kanálu pro přenosové fronty.

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

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

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

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

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

   Zobrazuje stav kanálu a hloubku přenosové fronty během přepnutí. Následující příklad zobrazuje stav přenosových front systémového klastru.

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

4. Volitelné: Monitorování zpráv "AMQ7341 Přenosová fronta pro kanál *ChannelName* byla přepnuta z fronty *QueueName* do *QueueName*" , která jsou zapsána do protokolu chyb správce front.

Přepnutí zastaveného odesílacího kanálu klastru do jiné přenosové fronty klastru

Než začnete

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

Pokud snížíte počet zpráv, které proces přepínání musí přenést do nové přenosové fronty, přechod bude rychlejší. Než budete pokračovat dále, přečtěte si “Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje” na stránce 170 , abyste zjistili důvody pro pokus o vyprázdnění přenosové fronty.

Informace o této úloze

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

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

Postup

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

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

2. Volitelné: Proveďte změny konfigurace.

   Například viz “Klastrování: Příklad konfigurace více přenosových front klastru” na stránce 283.
3. Přepněte odesílací kanály klastru na nové přenosové fronty klastru.

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

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

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

   Vzhledem k tomu, že kanál odesílatele klastru je zastaven, budou zprávy navazovat na novou přenosovou frontu. Porovnejte zastavený kanál odesílatele klastru, na krok “2” na stránce 293 v tématu “Přepínání aktivních odesílacích kanálů klastru na jinou sadu front-přenosových front” na stránce 292. V tomto kroku je kanál odesílatele klastru spuštěn, takže zprávy nemusí být nutně sestaveny v nové přenosové frontě.
4. Volitelné: Monitorování kanálů při přepnutí

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

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

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

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

   ```
   START CHANNEL(ChannelName)
   ```

Související odkazy
runswchl
Vyřešit kanál
Ukončit kanál

Klastrování: migrace a úprava doporučených postupů

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

1. “Přesun objektů v klastru” na stránce 295 (Nejlepší postupy pro přesouvání objektů v rámci klastru bez instalace oprav FixPack nebo nových verzí produktu IBM WebSphere MQ).
2. “Upgrade a údržba instalací” na stránce 296 (Nejlepší postupy pro udržení funkční architektury klastrů při použití údržby nebo přechodů na vyšší verzi a testování nové architektury).

Přesun objektů v klastru

Aplikace a jejich fronty

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

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

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

Přesun celých správců front

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

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

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

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

- Zacházet s celým procesem jako s obnovou správce front ze zálohy a aplikovat všechny procesy, které byste obvykle používali pro obnovu systému, jak je to vhodné pro prostředí operačního systému.
- Použijte příkaz **REFRESH CLUSTER** po migraci k vyřazení všech lokálně zadržovaných informací o klastru (včetně všech automaticky definovaných kanálů, které jsou nejisté) a vynuťte jeho opětovné sestavení.

Poznámka: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.

Při vytváření správce front a replikaci nastavení z existujícího správce front v klastru (jak je popsáno výše v tomto tématu) se nikdy nezpracují dva různé správce front jako ve skutečnosti stejné. Zejména nepojmenujte nového správce front se stejným názvem správce front a adresou IP. Pokus o 'zrušení' náhradního správce front je častou příčinou problémů v klastrech produktu IBM WebSphere MQ . Mezipaměť očekává přijetí aktualizací včetně atributu **QMID** a stav může být poškozen.

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

Upgrade a údržba instalací

Vyvarujte se scénáře "big bang" (například zastavení všech aktivit klastrů a správců front, použití všech upgradů a údržby pro všechny správce front a následné spuštění všeho najednou): Klastry jsou navrženy tak, aby stále pracovaly s více verzemi správce front, takže je doporučen dobře naplánovaný přístup pro údržbu po etapách.

Připravte si záložní plán:

- V produktu z/OSjste aplikovali zpětně migrování PTF?
- Zbali jste se zálohy?
- Vyvarovat se použití nových funkcí klastru okamžitě: Počkejte, až budete mít jistotu, že všichni správci front jsou upgradováni na novou úroveň a že jste si jisti, že se z nich nechystáte odvolat žádné. Použití nové funkce klastru v klastru, v němž jsou někteří správci front stále na nižší úrovni, může vést k nedefinovanému chování. Pokud například správce front definuje určité téma klastru, správce front produktu IBM WebSphere MQ Version 6.0 v přechodu na produkt IBM WebSphere MQ Version 7.1 z produktu IBM WebSphere MQ Version 6.0nerozumí definici nebo může být schopen publikovat na tomto tématu.

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

Související pojmy

“Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 296

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

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

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

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

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

Pokud se tyto informace nedostanete do správců front v klastru, kde je to vyžadováno, například klastrovaná fronta není známa jiným správcem front v klastru, když se aplikace pokusí ji otevřít poprvé, znamená to, že se jedná o problém v infrastruktuře klastru. Například je možné, že kanál nelze spustit

mezi správcem front a úplným správcem front úložiště. Proto musí být prošetřena každá situace, v níž jsou zjištěny nesrovnalosti. Je-li to možné, vyřešte situaci bez použití příkazu **REFRESH CLUSTER** .

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

Aktualizace ve velkém klastru může ovlivnit výkon a dostupnost klastru.

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

Pokud nelze použít alternativní metody a musíte spustit prostor **REFRESH CLUSTER** ve velkém klastru, měli byste to provést ve vypnutém čase nebo v průběhu okna údržby, abyste se vyhnuli vlivu na pracovní zátěže uživatelů. Měli byste se také vyhnout obnově velkého klastru v jedné dávce a místo toho, abyste aktivitu fázovali, jak je vysvětleno v tématu “Vyvarovat se problémů s výkonem a dostupností, když objekty klastru odesílají automatické aktualizace” na stránce 297.

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

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

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

Fronta historie systémového klastru

Je-li provedeno **REFRESH CLUSTER** , správce front pořídí snímek stavu klastru před obnovou a uloží jej na `SYSTEM.CLUSTER.HISTORY.QUEUE` (SCHQ), pokud je definován ve správci front. Tento snímek je určen pouze pro servisní účely produktu IBM , a to v případě pozdějších problémů se systémem. SCHQ je standardně definován u distribuovaných správců front při spuštění. V případě migrace produktu z/OS musí být SCHQ ručně definována. Platnost zpráv o SCHQ vyprší za tři měsíce.

Související pojmy

Problémy aplikace zaznamenané při spuštění REFRESH CLUSTER

Aspekty REFRESH CLUSTER pro klastry publikování/odběru

Související odkazy

Popis příkazů MQSC: REFRESH CLUSTER

Klastrování: Dostupnost, více instancí a zotavení z havárie

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

IBM WebSphere MQ Klastrování samo o sobě není řešením vysoké dostupnosti, ale za určitých okolností může být použito ke zlepšení dostupnosti služeb pomocí produktu IBM WebSphere MQ, například tím, že má více instancí fronty na různých správcích front. Tento oddíl poskytuje pokyny k zajištění co nejvyšší dostupnosti infrastruktury produktu IBM WebSphere MQ , aby bylo možné ji použít v takové architektuře.

Dostupnost prostředků klastru

Důvodem pro obvyklé doporučení k zachování dvou úplných úložišť je to, že ztráta jednoho z nich není kritická pro plynulé spouštění klastru. I když se obě stanou nedostupnými, existuje 60denní doba odkladu pro existující znalosti, které se nacházejí v částečných úložištích, ačkoli v této události nejsou k dispozici nové nebo dříve nedostupné prostředky (fronty pro příklad).

Použití klastrů ke zlepšení dostupnosti aplikací

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

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

Správci front s více instancemi

Software High Availability (multi-instance) je nejlepší vestavěná nabídka pro zachování dostupnosti stávajících zpráv. Další informace naleznete v části “Použití produktu WebSphere MQ s konfiguracemi vysoké dostupnosti” na stránce 307, “Vytvoření správce front s více instancemi” na stránce 335a v následující sekci. Jakýkoli správce front v klastru může být prostřednictvím této techniky vysoce dostupný, pokud jsou všichni správci front v klastru spuštění alespoň IBM WebSphere MQ Version 7.0.1. Jsou-li všichni správci front v klastru na předchozí úrovni, mohou ztratit konektivitu s správci front pro více instancí, pokud dojde k selhání na sekundární adresu IP.

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

Zotavení z havárie

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

- Dávejte pozor při testování scénářů zotavení z havárie. Pokud například testujete operaci se správci front zálohování, buďte opatrní při jejich uvedení do stavu online ve stejné síti, protože je možné náhodně připojit aktivní klastr a začít 'kradení' zpráv hostováním stejných pojmenovaných front jako v aktivních správcích front klastru.
- Testování zotavení z havárie nesmí kolidovat se spuštěným aktivním klastrem. Techniky zabraňování interferenci zahrnují:
  - Dokončete oddělování sítě nebo oddělení na úrovni brány firewall.
  - Do systému zotavení z havárie se nevydává aktuální certifikát SSL, nebo pokud se nevyskytne scénář zotavení z havárie.
- Když obnovujete zálohu správce front v klastru, je možné, že záloha nebude synchronizována se zbytkem klastru. Příkaz **REFRESH CLUSTER** může vyřešit aktualizace a synchronizovat s klastrem, ale příkaz **REFRESH CLUSTER** se musí použít jako poslední možnost. Viz “Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER” na stránce 296. Chcete-li zjistit, zda byl

před použitím příkazu použit jednoduchý krok, prostudujte si všechny interní dokumentaci procesu a dokumentaci produktu IBM WebSphere MQ .

- Pokud jde o jakékoli zotavení, aplikace se musí vypořádat s přehráním a ztrátou dat. Je třeba se rozhodnout, zda vymazat fronty do známého stavu, nebo pokud existuje dostatek informací pro správu přehraných informací.

Klastrování: monitorování

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

Monitorování zpráv aplikace v klastru

Zpravidla se všechny zprávy klastru, které opouštějí správce front, předávají prostřednictvím serveru SYSTEM.CLUSTER.TRANSMIT.QUEUEbez ohledu na to, který odesílací kanál klastru se používá k přenosu zprávy. Každý kanál provádí paralelní zpracování zpráv cílených pro daný kanál se všemi ostatními odesílacími kanály klastru. Rostoucí build-up zpráv v této frontě může indikovat problém s jedním nebo více kanály a musí být prozkoumán:

- Hloubka fronty musí být řádně monitorována pro návrh klastru.
- Následující příkaz vrací všechny kanály, které mají více než jednu zprávu čekající na přenosové frontě:

```
DIS CHSTATUS(*) WHERE(XQMSGSA GT 1)
```

  Se všemi zprávami klastru na jedné frontě není vždy snadné zjistit, který kanál má problémy, když se začne vyplňovat. Použití tohoto příkazu je snadný způsob, jak zjistit, který kanál je zodpovědný.

Správce front klastru můžete nakonfigurovat tak, aby měl více přenosových front. Změníte-li atribut správce front DEFCLXQ na hodnotu CHANNEL, bude každý kanál odesílatele klastru asociován s jinou přenosovou frontou klastru. Alternativně můžete nakonfigurovat samostatné přenosové fronty ručně. Chcete-li zobrazit všechny přenosové fronty klastru přidružené k odesílacím kanálům klastru, spusťte následující příkaz:

```
DISPLAY CLUSQMGR (qmgrName) XMITQ
```

Definujte přenosové fronty klastru tak, aby následování vzorku měly pevný základ názvu fronty na levé straně. Poté můžete dotázat se na hloubku všech přenosových front klastru navrácených příkazem **DISPLAY CLUSMGR** pomocí generického názvu fronty:

```
DISPLAY QUEUE (qname*) CURDEPTH
```

Monitorování řídicích zpráv v klastru

Fronta produktu SYSTEM.CLUSTER.COMMAND.QUEUE se používá ke zpracování všech řídicích zpráv klastru pro správce front, buď generovaných lokálním správcem front, nebo odeslaných tomuto správci front z jiných správců front v klastru. Pokud správce front správně udržuje svůj stav klastru, má tato fronta tendenci k nule. Existují situace, kdy hloubka zpráv v této frontě může dočasně růst:

- Počet zpráv ve frontě indikuje churn ve stavu klastru.
- Když provádíte významné změny, umožněte, aby se fronta usadila mezi těmito změnami. Pokud například přesouváte úložiště, před přesunutím druhého úložiště umožníte, aby se fronta dostala na nulu.

Zatímco v této frontě existují nevyřízené zprávy, aktualizace stavu klastru nebo příkazů souvisejících s klastrem se nezpracovávají. Pokud nejsou zprávy z této fronty již dlouho odstraněny, je zapotřebí další vyšetřování, nejprve kontrolou chyb správce front , což může vysvětlit proces, který tuto situaci způsobuje.

SYSTEM.CLUSTER.REPOSITORY.QUEUE uchovává informace o mezipaměti úložiště klastru jako počet zpráv. Je obvyklé, že zprávy vždy existují v této frontě, a více pro větší klastry. Proto není hloubka zpráv v této frontě důvodem k obavám.

Protokoly monitorování

Problémy, které se vyskytnou v klastru, nemusí zobrazit externí symptomy aplikací po mnoho dní (a dokonce měsíce) poté, co se problém původně vyskytl kvůli ukládání informací do mezipaměti a distribuovanému charakteru klastrování. Avšak původní problém je často hlášen v protokolech chyb IBM WebSphere MQ. Z tohoto důvodu je životně důležité aktivně monitorovat tyto protokoly pro všechny zprávy zapsané v souvislosti s klastrováním. Tyto zprávy je třeba číst a chápat, přičemž v případě potřeby musí být provedena jakákoli akce.

Například: přerušení komunikace se správcem front v klastru může mít za následek znalosti o určitých klastrových prostředcích, které se odstraňují kvůli tomu, že klastry pravidelně znovu ověřují prostředky klastru tím, že znovu publikují informace. Zpráva AMQ9465obsahuje varování o takové události, která může být potenciálně generována. Tato zpráva označuje, že problém musí být zjišťován.

Speciální aspekty vyrovnávání zátěže

Když klastr vyrovnává zátěž mezi dvěma nebo více instancemi fronty, musí spotřebovávající aplikace zpracovávat zprávy na každém z těchto instancí. Pokud se jedna nebo více těchto aplikací ukončuje nebo zastaví zpracování zpráv, je možné, že klastrování bude pokračovat v odesílání zpráv do těchto instancí fronty. V této situaci se tyto zprávy nezpracovávají, dokud aplikace nebudou znovu fungovat správně. Z tohoto důvodu je monitorování aplikací důležitou součástí řešení a musí být přijata opatření k přesměrování zpráv v této situaci. Příklad mechanizmu pro automatizaci takového monitorování lze nalézt v této ukázce: Ukázkový program pro monitorování front klastru (AMQSCLM) .

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

Na platformách Windows, UNIX, Linux a IBM i implementujte 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 tato aktivní instance, selže, je provedení automaticky přepnuto na instanci v pohotovostním režimu téhož 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 WebSphere MQ můžete nakonfigurovat jako součást klastrovacího řešení specifického pro platformu, jako je například Microsoft Cluster Server, nebo PowerHA pro systém AIX (dříve HACMP na systému AIX) a další klastrová řešení UNIX and Linux .

Další možností, 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 WebSphere MQ může trasovat přenosovou cestu zprávy 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 WebSphere MQ zajišťuje, že zprávy nebudou ztraceny udržováním žurnálů pro zotavení aktivit správců front, kteří zpracovávají zprávy o příjmu, přenosu a doručování zpráv.Využívá tyto protokoly pro tři typy obnovy:

1. *Opětovné spuštění zotavení*při zastavení produktu WebSphere MQ v plánovaném způsobu.
2. *Zotavení po selhání*, při zastavení serveru WebSphere 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 *vložené*. Toto připojení se automaticky obnoví v každém okamžiku aplikačního programu klienta a obnoví se všechny popisovače k otevřeným objektům.

Naproti tomu manuální opětovné připojení vyžaduje aplikaci klienta k opětovnému vytvoření připojení pomocí `MQCONN` nebo `MQCONNX`a k opětnému otevření objektů. Automatické opětovné připojení klienta je vhodné pro řadu aplikací klienta, nikoliv však pro všechny.

Tabulka 28 na stránce 301 uvádí nejstarší vydání podpory klienta IBM WebSphere 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 29 na stránce 302 vypíše další požadavky, které umožní automatické opětovné připojení klienta.

Při přístupu programu k volbám opětovného připojení může klientská aplikace nastavit možnosti opětovného připojení. Pokud má klientská aplikace přístup k volbám opětovného připojení, kromě klientů JMS a XMS , může také vytvořit obslužnou rutinu událostí pro zpracování událostí opětovného připojení.

Existující klientská aplikace může mít prospěch z podpory opětovného připojení, bez rekompilace a linkování:

- Pro jiného klienta než JMS nastavte proměnnou prostředí `mqclient.ini` `DefRecon` tak, aby nastavila možnosti opětného 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 JMS nastavte volby opětovného připojení v konfiguraci továrny připojení. Používáte-li adaptér prostředků WebSphere MQ nebo klienta JMS, který je integrován v prostředí Java EE , automatické opětovné připojení klienta nemusí být k dispozici. Některá ze spravovaných prostředí obsahuje omezení, další informace viz téma Použití automatického opětovného připojení klienta v prostředí Java SE a Java EE.

Poznámka: Automatické opětovné připojení klienta není podporováno třídami produktu WebSphere MQ pro prostředí Java.

Tabulka 28. Podporovaní klienti

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 v systému Windows)	7.0.1	7.0.1
	Kontejner klienta JMS (JSE a kontejner klienta Java EE a spravované kontejnery)	7.0.1.3	7.0.1.3
	Třídy WebSphere MQ pro jazyk Java	Nepodporováno	Nepodporováno
	Spravované klienty XMS a spravované klienty .NET: C#, Visual Basic.	7.1	7.1

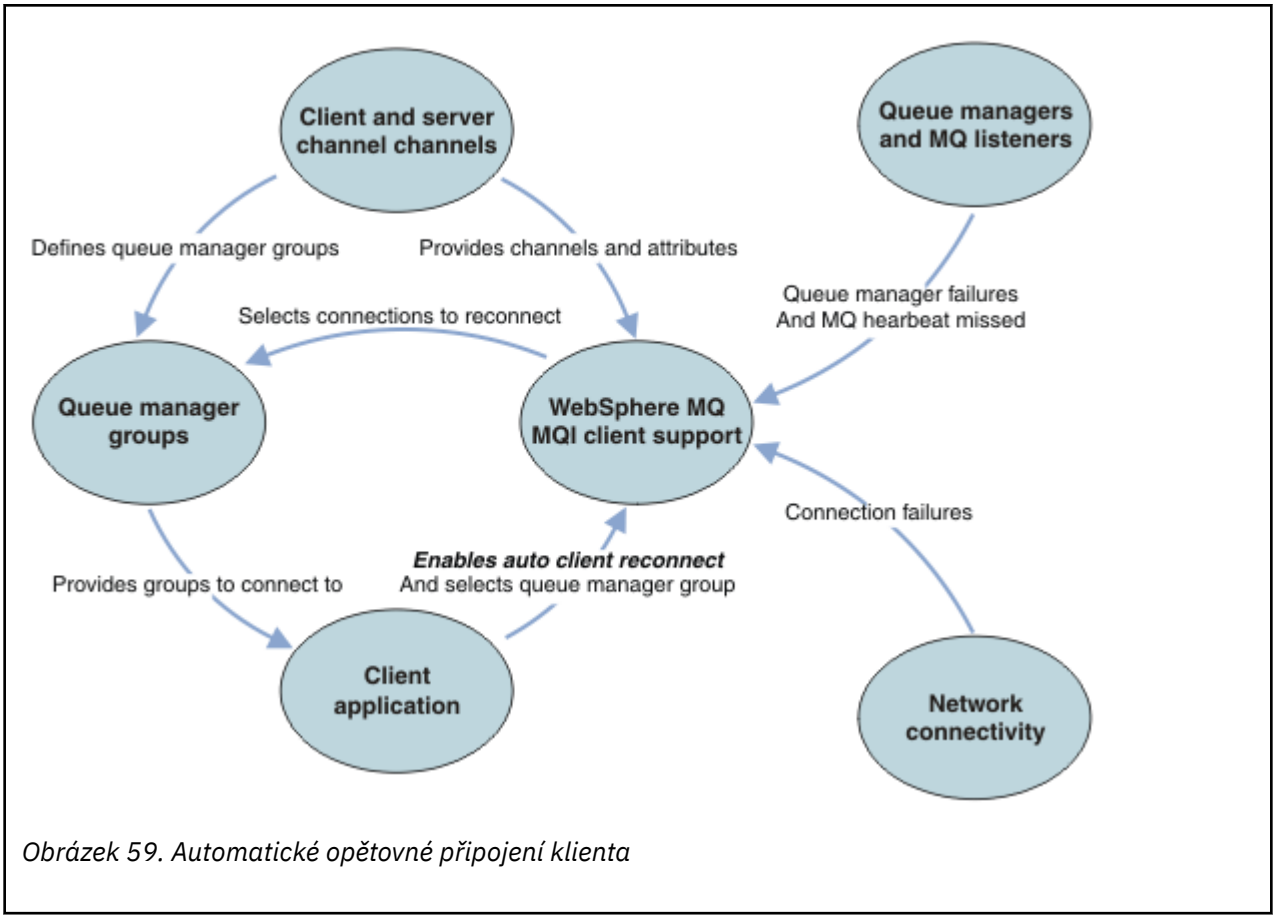
Tabulka 28. Podporovaní klienti (pokračování)			
Rozhraní klienta	**Klient**	**Přístup k programu pro volby opětovného připojení**	**Podpora opětovného připojení**
Jiná rozhraní API	Windows Communication Foundation (Nespravovaný[1])	Nepodporováno	7.0.1
	Windows Communication Foundation (Spravováno[1])	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:

Tabulka 29. Požadavky na konfiguraci automatického opětovného připojení		
Komponenta	**Požadavek**	**Vliv nesplnění požadavku**
Instalace klienta WebSphere MQ MQI	Viz Tabulka 28 na stránce 301	`MQRC_OPTIONS_ERROR`
Instalace serveru WebSphere MQ Server	Úroveň 7.0.1	`MQRC_OPTIONS_ERROR`
Kanál	`SHARECNV > 0`	`MQRC_ENVIRONMENT_ERROR`
prostředí aplikace	Musí být vláknový	`MQRC_ENVIRONMENT_ERROR`
MQI	Jedna z možností: • `MQCONNX` s volbami `MQCNE` `Volby` nastaveným na hodnotu `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR`. • `Defrecon=YES|QMGR` je v `mqclient.ini` • Ve službě JMS nastavte vlastnost CLIENTRECONOPTIONS továrny na připojení.	`MQCC_FAILED` je-li připojení přerušeno nebo selže nebo selže správce front.

Produkt Obrázek 59 na stránce 303 zobrazuje hlavní interakce mezi komponentami, které jsou zapojeny do opětovného připojení klienta.



Obrázek 59. Automatické opětovné připojení klienta

Aplikace klienta

Klientská aplikace je klientem IBM WebSphere MQ MQI.

- Ve výchozím nastavení nejsou klienti automaticky znovu připojeni. Povolte automatické opětovné připojení klienta nastavením volby `MQCONNX` `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 380.
- 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 (s MQPUT a MQPUT1) nebo MQGMO_LOGICAL_ORDER (s MQGET) při nastavení voleb opětného 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 klientských aplikací WebSphere MQ MQI 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 klienti WebSphere MQ MQI znovu připojují k libovolnému správci front ve skupině správců front. Někdy chcete, aby se klient WebSphere MQ MQI znovu připojil pouze ke stejnému správci front. Může mít afinitu ke správci front. Klienta můžete zabránit tak, aby se znovu připojli k jinému správci front. Nastavte volbu MQCNO , MQCNO_RECONNECT_Q_MGR. Klient WebSphere MQ MQI se nezdaří, pokud se znovu připojí k jinému správci front. 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 kterémkoli 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 systému z/OS používá stejné mechanizmy 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 položky v tabulce byly interpretovatelné ve stejné skupině sdílení front systému 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)KAINT
Interval udržení aktivity. Nastavte interval udržení aktivity na kanálu připojení serveru.

Všimněte si, že KAINT platí pouze pro operační systém 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 (KAINT)KAINT
Interval udržení aktivity. Nastavte interval udržení aktivity na kanálu připojení klienta.

Všimněte si, že KAINT platí pouze pro operační systém z/OS .

KAINT je prezenční signál síťové vrstvy a HBINT je prezenční signál produktu WebSphere 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 síťového 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 KAINT 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 předána klientovi WebSphere MQ MQI klientem, jsou obsluhována schopností automatického opětovného připojení klienta.

- Opětovné připojení provedená automaticky přenosem je neviditelná pro IBM WebSphere MQ.
- Nastavení hodnoty HBINT pomáhá řešit selhání sítě, která jsou neviditelná pro produkt WebSphere MQ.

Správci front a moduly listener produktu WebSphere 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 klienta WebSphere MQ MQI

Použijete-li v klientu WebSphere MQ MQI podporu automatického připojení klienta, klientská aplikace se automaticky znovu připojí a pokračuje ve zpracování bez zadání volání MQCONN nebo MQCONNX MQI, aby se znovu připojil 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 382.
- 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 opětovné připojení trvá déle než jednu minutu, opětovné připojení může trvat déle, protože správce front může mít mnoho prostředků ke správě. Během této doby může aplikace klienta obsahovat zámky, které nenáleží k prostředkům produktu WebSphere 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 potenciálně potřebuje adresování.

Přítomnost této zprávy může také označovat, že uživatelská aplikace vkládá do sady stránek velký počet zpráv, což může být příznakem většího problému:

- Problém s uživatelskou aplikací, která odesílá zprávy PUT, jako např. neřízenou smyčku.
- Uživatelská aplikace, která GET zprávy z fronty, již nefunguje.

Použití produktu WebSphere MQ s konfiguracemi vysoké dostupnosti

Chcete-li provozovat správce front produktu WebSphere MQ v konfiguraci vysoké dostupnosti (HA), můžete nastavit správce front tak, aby pracoval buď se správcem vysoké dostupnosti, jako je například produkt PowerHA pro systém AIX (dříve HACMP) nebo služba Microsoft Cluster Service (MSCS), nebo se správci front WebSphere 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, které jsou vzájemně propojeny a konfigurovány tak, že pokud jedna selže, správce vysoké dostupnosti, jako například HACMP (UNIX) nebo MSCS (Windows), provede *překonání selhání*. Překonání selhání přenese 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 WebSphere MQ a klastry HA je popsán v tématu "Vztah klastrů s vysokou dostupností do klastrů správců front" na stránce 308.

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 zasílání zpráv založené na produktu WebSphere MQ, aniž byste potřebovali technologii klastrů, jako je například produkt 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 WebSphere MQ
- Rychlejší překonání selhání než klastr HA
- Jednoduchá konfigurace a operace
- Integrace s produktem WebSphere 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 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 přeživím 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.

Použití produktu WebSphere MQ s klastrem s vysokou dostupností v systému UNIX and Linux

Můžete použít produkt WebSphere MQ s klastrem s vysokou dostupností (HA) na platformách UNIX and Linux : například produkt PowerHA pro systém AIX (dříve HACMP), Veritas Cluster Server, HP Serviceguard nebo Red Hat Enterprise Linux klastr s Red Hat Cluster Suite.

Před verzí produktu WebSphere MQ verze 7.0.1byla poskytnuta sada SupportPac MC91 , která byla nápomocna při konfigurování klastrů s vysokou dostupností. Produkt WebSphere MQ verze 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 308, vztah klastrů s vysokou dostupností do klastrů správců front, “Klienti produktu WebSphere MQ” na stránce 309a “WebSphere MQ fungující v klastru s vysokou dostupností” na stránce 309, 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 WebSphere MQ můžete použít k nastavení rezervní nebo převzatelné konfigurace, včetně vzájemného převzetí, kde všechny uzly klastru používají pracovní zátěž produktu WebSphere MQ .

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 nepřenosné 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 přeživím 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.

Klienti produktu WebSphere MQ

Klienti produktu WebSphere MQ komunikující se správcem front, kteří mohou být předmětem restartování nebo převzetí, musí být napsány tak, aby tolerovali přerušené připojení a opakovaně se musí pokusit o připojení znovu. Produkt 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.

Klient rozšířených transakcí (ETC), který umožňuje použití klienta WebSphere MQ MQI k účasti ve dvoufázových transakcích, musí být vždy připojen ke stejnému správci front. ETC nemůže použít techniky, jako je prostředek pro vyrovnávání zatížení IP k výběru ze seznamu správců front. Pokud používáte produkt HA, udržuje správce front svou identitu (název a adresa), na kterémkoliv uzlu běží, takže ETC lze použít se správci front, kteří jsou pod kontrolou funkce HA.

WebSphere MQ fungující 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:

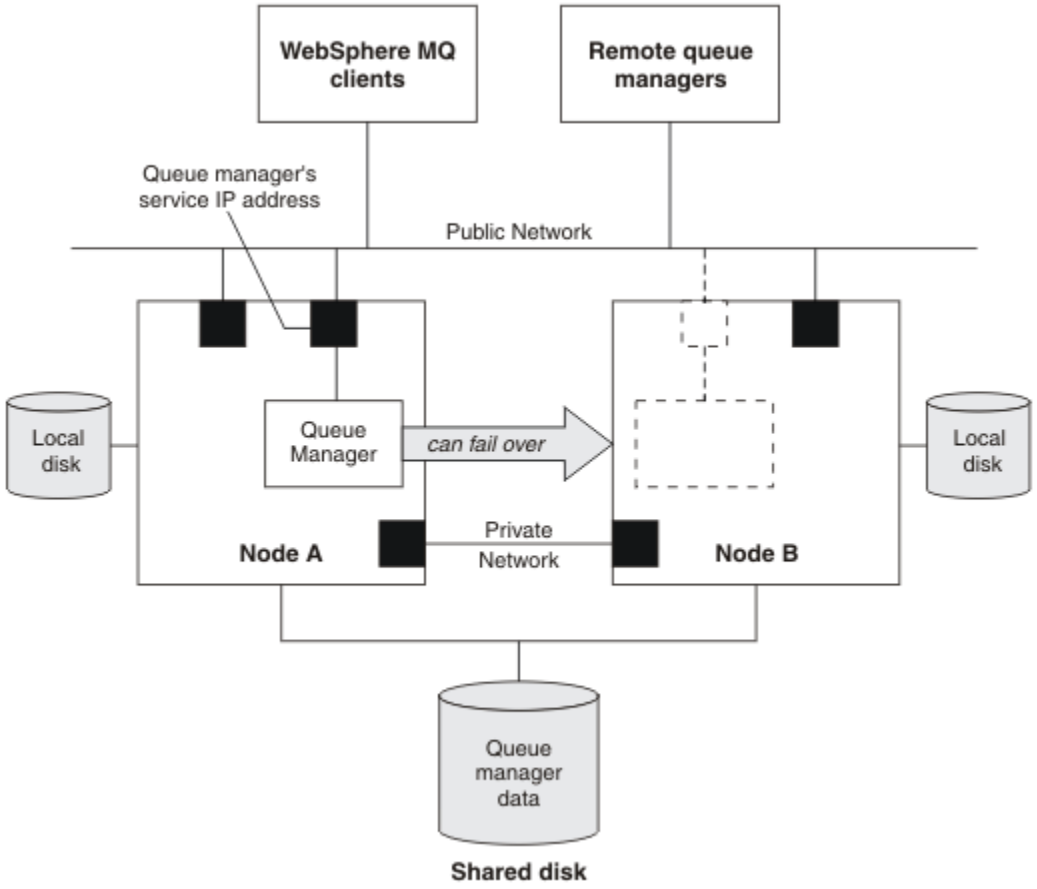
- V produktu PowerHA pro systém AIX se jednotka překonání selhání nazývá *skupina prostředků*.
- Na serveru Veritas Cluster Server je znám jako *skupina služeb*.
- Na Serviceguard se nazývá *balík*.

Toto téma používá termín *skupina prostředků* k označení jednotky překonání selhání.

Nejmenší jednotka překonání selhání pro produkt WebSphere 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 další prostředky WebSphere MQ , jako např. modul listener nebo monitor spouštěčů ve stejné skupině prostředků, buď jako oddělené 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. Klastr HA zajišťuje, že v daném okamžiku může zapisovat na disky pouze jeden uzel v klastru. Klastr 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 60. Klastr vysoké dostupnosti

Obrázek 1 ilustruje klastr s vysokou dostupností se dvěma uzly. Klastr 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 klastrem HA. Správce front závisí na sdíleném disku a na jeho adrese IP služby. Selže-li klastr 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 klastr s vysokou dostupností obsahuje více než jednoho správce front, může konfigurace klastru s vysokou dostupností vést ke spuštění dvou nebo více správců front spuštěných ve stejném uzlu po překonání selhání. Každému správci front v klastru s vysokou dostupností musí být přiřazeno vlastní číslo portu, které používá v libovolném uzlu klastru, který má být aktivní v libovolném konkrétním čase.

Obecně je klastr vysoké dostupnosti spuštěn jako uživatel root. Produkt WebSphere MQ se spouští jako uživatel mqm. Administrace produktu WebSphere MQ je přidělena členům skupiny mqm. Ujistěte se, že uživatel mqm a skupina existují na všech uzlech klastru vysoké dostupnosti. ID uživatele a ID skupiny musí být konzistentní v rámci klastru. Administrace produktu WebSphere MQ uživatelem root není povolena; skripty, které spouštějí, zastavují nebo monitorují skripty, se musí přepnout na uživatele mqm.

Poznámka: Produkt WebSphere MQ musí být na všech uzlech správně instalován; nelze sdílet spustitelné soubory produktu.

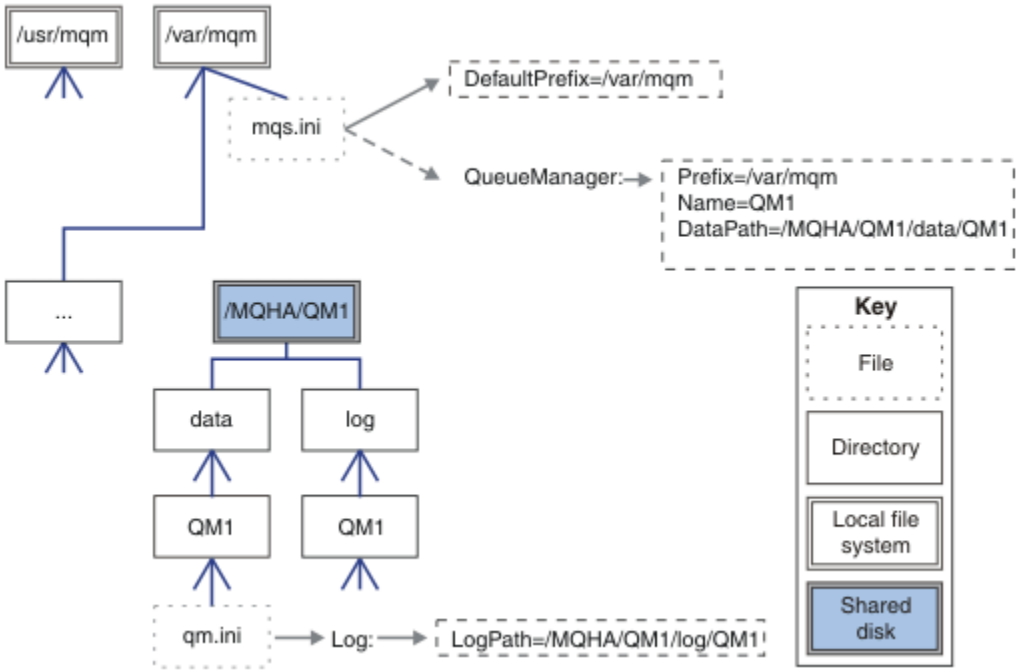
Konfigurace sdílených disků

Správce front WebSphere 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 61. 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 **dspmqinf** 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 312:

   ```
   dspmqinf -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 části “Přidání konfiguračních informací správce front do jiných uzlů v klastru s vysokou dostupností (HA)” na stránce 312.

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 311.

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 **dspmqinf** v krocích 6 a 7 v části “Vytvoření správce front pro použití v klastru s vysokou dostupností (HA)” na stránce 311.
3. Spuštěním a zastavením správce front ověřte konfiguraci.

   Příkazy použité ke spuštění a zastavení správce front musí být zadány ze stejné instalace IBM WebSphere 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 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
               amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
               amqzfuma amqzdmaa 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

# 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; 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 části “Spuštění správce front pod kontrolou klastru s vysokou dostupností (HA)” na stránce 312):

```
#!/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 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
                   amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
                   amqzfuma amqzdmaa 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 *.*$"
     cnt=`ps -ef | tr "\t" " " | grep amqzxma0 | grep -v grep | \
       egrep "$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
```

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 WebSphere MQ verze 7.1je možné mít v systému více instalací produktu WebSphere MQ . Další informace o více instalacích najdete v tématu Více instalací. Hodláte-li používat skript monitorování

přes více instalací, včetně instalací ve verzi 7.1nebo vyšší, budete možná muset provést několik dalších kroků. Pokud máte primární instalaci, nebo používáte skript s verzemi dřívějšími než verze 7.1, nemusíte pro použití skriptu zadávat*MQ_INSTALLATION_PATH* . Jinak následující kroky zajišťují, že je komponenta *MQ_INSTALLATION_PATH* správně identifikována:

1. Použijte příkaz **crtmqenv** z instalace verze 7.1 k identifikaci správného produktu *MQ_INSTALLATION_PATH* pro správce front:

   ```
   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: Produkt 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. Níže je uveden příklad skriptu použitého v systému AIX k zapouzdření názvu správce front:

```
#!/bin/ksh
su mqm -c name_of_monitoring_script qmname MQ_INSTALLATION_PATH
```

kde *MQ_INSTALLATION_PATH* je volitelný parametr, který uvádí cestu k instalaci produktu IBM WebSphere MQ , ke které je přidružen správce front *qmname* .

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 spouštěním 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 312):

```
#!/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 strmqm | 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 služby Microsoft Cluster Service (MSCS)

Zavedení a nastavení serveru MSCS pro podporu překonání selhání virtuálních serverů.

Tyto informace se týkají pouze produktu WebSphere MQ for Windows .

Služba MSCS (Microsoft Cluster Service) 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 přerušenou aplikaci řádným způsobem, přenese 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 317
- “Nastavení produktu IBM WebSphere MQ pro klastrování MSCS” na stránce 318

Poté se dozvíte, jak nakonfigurovat produkt WebSphere MQ pro klastrování MSCS, v následujících sekcích:

- “Vytvoření správce front pro použití se službou MSCS” na stránce 320
- “Přesun správce front do úložiště MSCS” na stránce 321
- “Vložení správce front do ovládacího prvku MSCS” na stránce 322
- “Odebrání správce front z ovládacího prvku MSCS” na stránce 328

Poté jsou uvedeny některé užitečné pokyny k použití prostředí MSCS s produktem WebSphere MQa podrobné informace o obslužných programech podpory WebSphere MQ MSCS v následujících sekcích:

- “Rady a tipy pro použití MSCS” na stránce 330
- “IBM WebSphere MQ programy obslužného programu pro podporu MSCS” na stránce 332

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.

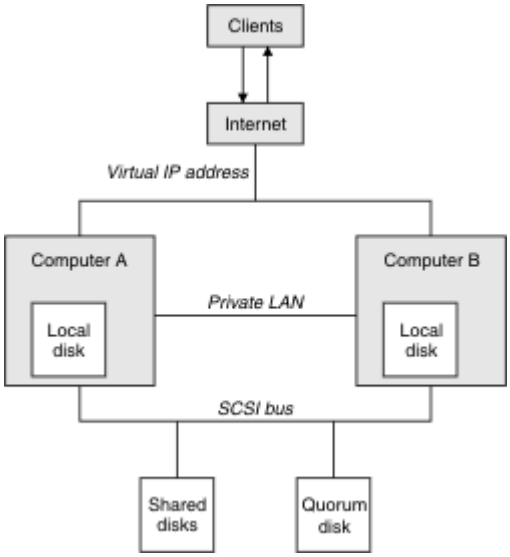
“Použití produktu WebSphere MQ s konfiguracemi vysoké dostupnosti” na stránce 307 obsahuje porovnání mezi klastry MSCS, správci front s více instancemi a klastry WebSphere MQ .

V této sekci a v jejích podřízených tématech výraz *cluster*, je-li používán samostatně, **vždy** znamená klastr MSCS. Tato funkce se liší od klastru WebSphere MQ popsaného 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*) Level 1, pro výhradní použití MSCS; je to znám jako disk *kvorum* . 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 přerušenou aplikaci řádným způsobem, přenese 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 dvoupočítačový klastr je zobrazeno v části Obrázek 62 na stránce 318.



Obrázek 62. 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 klastrem, si je vědom pouze jedné *virtuální adresy IP*a služba MSCS směruje 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 WebSphere MQ pro klastrování MSCS

Nakonfigurujte produkt IBM WebSphere 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 WebSphere MQ na každém počítači v klastru.

Vzhledem k tomu, že správce front je přidružen k názvu instalace produktu IBM WebSphere MQ , musí být název instalace produktu IBM WebSphere 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 WebSphere MQ; viz “Přesun správce front do úložiště MSCS” na stránce 321. Chcete-li vytvořit nové správce front pro použití se službou MSCS, přečtěte si téma “Vytvoření správce front pro použití se službou MSCS” na stránce 320.

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 322.

Pokud se rozhodnete odebrat správce front z ovládacího prvku MSCS, použijte proceduru popsanou v tématu “Odebrání správce front z ovládacího prvku MSCS” na stránce 328.

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 319.

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. To platí automaticky, pokud již máte doménu a účty vztahující se k produktu WebSphere 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 WebSphere MQ MSCS zajistí, aby všechny soubory, které obsahují objekty správce front, měly ekvivalentní oprávnění 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 WebSphere MQ můžete použít doménový účet. 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 produktem WebSphere MQ: Active/Passive nebo Active/Active.

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 umístěte 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 produkt WebSphere MQ to znamená, že můžete například spustit dva správce front, jeden na každém z A a B, přičemž každá z nich využívá úplnou 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.

Začneš tím, že vytvoříte správce front se všemi jeho prostředky na lokální jednotce a poté migrujte 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 WebSphere MQ Explorer. 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 WebSphere 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 změníte toto nastavení, znovu zaveďte systém počítače, aby se při změně došlo k jeho změně. Pokud proměnnou nenastavíte, bude správce front vytvořen ve výchozím adresáři produktu WebSphere MQ pro správce front.
2. Vytvořte správce front pomocí příkazu **crtmqm** . Chcete-li například vytvořit správce front s názvem `mscs_test` ve výchozím adresáři, použijte:

   ```
   crtmqm mscs_test
   ```

3. Pokračujte “Přesun správce front do úložiště MSCS” na stránce 321.

Vytvoření správce front pomocí Průzkumníka WebSphere MQ

Chcete-li pomocí Průzkumníka IBM WebSphere MQ vytvořit správce front pro použití se službou MSCS, postupujte takto:

1. Spusťte Průzkumníka IBM WebSphere 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 321.

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\<QMname>` a `C:\WebSphere MQ\qmgrs\<QMname>`. ***ne*** se snaží soubory přesunout ručně; použijte obslužný program dodávaný jako součást podpory MSCS produktu WebSphere 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, do kterého je produkt WebSphere MQ nainstalován. Příkaz `hamvmqm` neupravuje tento atribut správce front. V této situaci je třeba upravit atribut správce front, SSLKEYR, pomocí Průzkumníka IBM WebSphere 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 322.
3. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (informace o tom, proč je to důležité), najdete v tématu “Soubory protokolu správce front” na stránce 331 .
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:\
   WebSphere MQ" /ld "e:\
   WebSphere MQ\log"
   ```

   nahrazení názvu správce front názvem *qmname*, písmeno sdílené diskové jednotky pro *e*a vámi zvolený adresář pro produkt *WebSphere MQ*. Adresáře se vytvoří, pokud ještě neexistují.
8. Otestujte správce front, abyste se ujistili, že funguje, pomocí Průzkumníka IBM WebSphere 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 WebSphere MQ se ujistěte, že je atribut spuštění správce front nastaven na ruční zpracování. V Průzkumníku IBM WebSphere MQ nastavte pole spuštění na hodnotu `manual` v panelu vlastností správce front.
10. Pokračujte “Vložení správce front do ovládacího prvku MSCS” na stránce 322.

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 WebSphere 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 WebSphere MQ pro klastrování MSCS” na stránce 318.
2. Obslužný program **haregtyp** použijte k registraci produktu WebSphere MQ jako typ prostředku MSCS na všech uzlech klastru. Další informace naleznete v dokumentu “IBM WebSphere MQ programy obslužného programu pro podporu MSCS” na stránce 332 .
3. Pokud jste správce front dosud nevytvořili, přečtěte si téma “Vytvoření správce front pro použití se službou MSCS” na stránce 320.
4. Pokud jste správce front vytvořili nebo již existuje, ujistěte se, že jste tento postup provedli v produktu “Přesun správce front do úložiště MSCS” na stránce 321.
5. Zastavte správce front, je-li spuštěný, a to buď pomocí příkazového řádku, nebo pomocí Průzkumníka IBM WebSphere MQ .
6. Před přechodem na následující procedury systému Windows v tomto tématu otestujte operaci MSCS sdílených jednotek.

Windows Server 2012.

Upozornění: Podpora MSCS je dodávána v produktu WebSphere MQ 7.5 s 32bitovou knihovnou DLL. Kvůli omezení v systému Windows 2012 nedojde k překonání selhání správce front produktu IBM WebSphere MQ po restartu.

Společnost Microsoft nedoporučuji použití 32bitových knihoven DLL s operačním systémem Windows 2012, a proto není pro tuto záležitost momentálně k dispozici žádná oprava operačního systému. IBM neposkytuje 64bitovou knihovnu pro produkt IBM WebSphere MQ 7.5.

Od produktu IBM MQ 8.0 je k dispozici 64bitová knihovna, takže je nutné použít tuto verzi produktu pro plnou funkčnost MSCS s operačním systémem Windows 2012 a novějším.

Chcete-li umístit správce front pod řídicí prvek MSCS na server Windows Server 2012, postupujte takto:

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 používaného v produktu MSCS Cluster Administrator v předchozích verzích systému Windowspoužívá 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 přídavnou adresu, která je mezi nimi *floats* . Ačkoli služba MSCS zpracovává směrování této adresy, **neověřuje** , zda je adresa dosažitelná.
   d. Přiřaďte 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 nespoléhá 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 **IBM MQSeries MSCS** na panelu "Vybrat typ prostředku".
   f. Proveďte zbývající kroky v průvodci.
5. Před přivedení prostředku do stavu online potřebuje prostředek MSCS IBM MQSeries další konfiguraci:
   a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'Nový IBM MQSeries MSCS'.
   b. Klepněte pravým tlačítkem myši na položku **Vlastnosti** v prostředku MQ .
   c. Konfigurujte prostředek:
      - `Name`; zvolte název, který usnadňuje identifikaci správce front, pro kterého je určen.
      - `Run in a separate Resource Monitor`; pro lepší izolaci
      - `Possible owners`; nastavte oba uzly
      - `Dependencies`; přidejte diskovou jednotku a adresu IP pro tohoto správce front.

Varování: Selhání při přidávání těchto závislostí znamená, že produkt IBM WebSphere 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 WebSphere MQ mohou být zablokovány ze spuštění.

- `Parameters`; viz následující:
  - `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 332.
  - `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 332.

    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 328.

d. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu "Použití preferovaných uzlů" na stránce 332).

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 zátěži. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM WebSphere 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 321.) Můžete také klepnout pravým tlačítkem myši a vybrat volbu `Initiate Failure`; akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows Server 2008.

Chcete-li umístit správce front pod ovládací prvek MSCS na systému Windows Server 2008, postupujte takto:

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 > Spravovat klastr ...** k otevření připojení ke klastru.
4. Na rozdíl od schématu skupiny používaného v produktu MSCS Cluster Administrator v předchozích verzích systému Windowspoužívá 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 **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 přídavnou adresu, která je mezi nimi *floats* . Ačkoli služba MSCS zpracovává směrování této adresy, **neověřuje** , zda je adresa dosažitelná.
   d. Přiřaďte 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 nespoléhá 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 **IBM MQSeries MSCS** na panelu "Vybrat typ prostředku".
   f. Proveďte zbývající kroky v průvodci.
5. Před přivedení prostředku do stavu online potřebuje prostředek MSCS IBM MQSeries další konfiguraci:
   a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'Nový IBM MQSeries MSCS'.
   b. Klepněte pravým tlačítkem myši na položku **Vlastnosti** v prostředku MQ .
   c. Konfigurujte prostředek:
      - `Name`; zvolte název, který usnadňuje identifikaci správce front, pro kterého je určen.
      - `Run in a separate Resource Monitor`; pro lepší izolaci
      - `Possible owners`; nastavte oba uzly
      - `Dependencies`; přidejte diskovou jednotku a adresu IP pro tohoto správce front.

        Varování: Selhání při přidávání těchto závislostí znamená, že produkt WebSphere 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 WebSphere MQ mohou být zablokovány ze spuštění.

- Parameters; viz následující:
  - 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 332.
  - 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 332.

    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 328.

d. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu "Použití preferovaných uzlů" na stránce 332).

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 zátěži. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM WebSphere 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 Messagea 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 321.) Můžete také klepnout pravým tlačítkem myši a vybrat volbu Initiate Failure; akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows 2003.

Chcete-li umístit správce front pod ovládací prvek MSCS v systému 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 319.

   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 nespoléhá 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 přídavnou 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 WebSphere MQ MSCS*. Průvodce vás vyzve k zadání různých položek, včetně následujících:

   - `Name`; zvolte 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`; nastavte oba uzly
   - `Dependencies`; přidejte diskovou jednotku a adresu IP pro tohoto správce front.

     Varování: Selhání při přidávání těchto závislostí znamená, že produkt WebSphere 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 WebSphere MQ mohou být zablokovány ze spuštění.
   - `Parameters`; viz následující:
     - `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 332.
     - `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 332.

       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 328.

8. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si poznámky v části “Použití preferovaných uzlů” na stránce 332).
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 WebSphere 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 kdykoli chcete rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v tématu “Přesun správce front do úložiště MSCS” na stránce 321.) Můžete také klepnout pravým tlačítkem myši a vybrat volbu `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 odebíraný správce front používá připojení SSL, musíte upravit atribut správce front, SSLKEYR, pomocí Průzkumníka WebSphere MQ nebo příkazu MQSC `ALTER QMGR`tak, 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 329 .
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 329.
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 volbu `Groups`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 disk počítače, tj. stane se z něj *běžný* správce front WebSphere 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\qmgrs\<QMname>`. Nepokoušejte se soubory ručně přesunout; použijte obslužný program **hamvmqm** dodaný jako část podpory WebSphere MQ MSCS:

1. Ukončete činnost správce front a zkontrolujte, zda nedošlo k žádným chybám.
2. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (informace o tom, proč je to důležité), najdete v tématu “Soubory protokolu správce front” na stránce 331 .
3. Rozhodněte se, kterou lokální jednotku chcete použít, a ujistěte se, že má dostatečnou kapacitu pro ukládání souborů protokolu správce front a datových souborů (fronty).
4. 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.
5. Spusťte obslužný program k přesunutí správce front následujícím způsobem:

   ```
   hamvmqm /m qmname /dd "c:\
   WebSphere MQ" /ld "c:\
   WebSphere MQ\log"
   ```

   nahrazení názvu správce front *qmname*, písmeno vaší lokální diskové jednotky pro *c*a vámi zvolený adresář pro produkt *WebSphere MQ* (adresáře se vytvoří, pokud ještě neexistují).
6. Otestujte správce front a ujistěte se, že pracuje (jak je popsáno v tématu “Přesun správce front do úložiště MSCS” na stránce 321).

Rady a tipy pro použití MSCS

Tento oddíl obsahuje některé obecné informace, které vám pomohou efektivně využívat podporu produktu WebSphere MQ pro službu MSCS.

Tento oddíl obsahuje některé obecné informace, které vám pomohou efektivně využívat podporu produktu WebSphere 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. Testy IBM ukázaly překonání selhání a odvolání při selhání přibližně jedné minuty. 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 320 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 MSCS produktu WebSphere MQ může restartovat službu IBM MQSeries bez okamžitého spuštění správce front.

Podpora WebSphere 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 321.

MSCS a správce front
Aspekty týkající se správců front při použití MSCS.

Vytvoření odpovídajícího správce front v jiném uzlu

Pro práci s klastry pro práci s produktem WebSphere MQje pro každý uzel na uzlu B zapotřebí identického správce front v uzlu B. 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 321, 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 WebSphere 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 popsaný v tématu “IBM WebSphere MQ programy obslužného programu pro podporu MSCS” na stránce 332 , 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 62 na stránce 318). 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 320
- “Přesun správce front do úložiště MSCS” na stránce 321
- “Vložení správce front do ovládacího prvku MSCS” na stránce 322

Vykazování MSCS, které správci front mají spravovat

Vybíráte, kteří správci front jsou umístěními 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 321).

Před přesunem je vhodné správce front řádně vypnout a provést úplné zálohování datových souborů a souborů protokolu.

Více správců front

Podpora MSCS produktu WebSphere MQ 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 WebSphere MQ . Místo toho použijte administrátora klastru MSCS k převedení správce front do režimu online nebo jej převeďte 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 spouštění 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** používat aktivní režim Active/Active. Je tomu tak proto, že pro použití produktu WebSphere MQ s MSCS a COM +:

- Aplikační komponenty, které používají podporu COM + produktu WebSphere MQ, musí být spuštěny na stejném počítači jako koordinátor distribuovaných transakcí (DTC), což je 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
Use these commands to integrate WebSphere MQ MSCS support with other systems. Můžete je použít k vydání příkazů produktu WebSphere MQ , což je omezení některých omezení.

Určete tyto příkazy v parametrech pro prostředek typu `IBM WebSphere MQ MSCS`. Můžete je použít k integraci podpory MSCS produktu WebSphere 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. Když jsou tyto příkazy vyvolány, jsou standardně spuštěny z adresáře systému Windows. Vzhledem k tomu, že produkt WebSphere MQ používá 32bitový proces monitorování prostředků, v 64bitových systémech Windows se jedná o adresář `\Windows\SysWOW64` , nikoli na adresář `\Windows\system32`. Další informace naleznete v dokumentaci 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; podpora WebSphere MQ MSCS před pokračováním nebude čekat na dokončení těchto příkazů. Tím vyloučíte jakékoli riziko, že by mohly blokovat nebo zpožďovat další operace klastru.

Tyto příkazy můžete také použít k zadání příkazů produktu WebSphere MQ , například pro 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 vyskytli 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 WebSphere 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 WebSphere MQ v prostředí Microsoft Cluster Server (MSCS) v případě, že nebyl v takovém prostředí nakonfigurován Microsoft Distributed Transaction Coordinator (MSDTC). Informace o konfiguraci MSDTC v klastrovaném prostředí najdete v dokumentaci společnosti Microsoft .

IBM WebSphere MQ programy obslužného programu pro podporu MSCS
Seznam podpory IBM WebSphere MQ pro obslužné programy MSCS, které můžete spustit na příkazovém řádku.

Podpora produktu IBM WebSphere MQ pro službu MSCS zahrnuje následující obslužné programy:

Registrace/zrušení registrace typu prostředku
`haregtyp.exe`

Po *zrušení registrace* typu prostředku IBM WebSphere 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 produktu MSCS Cluster Administrator 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 329.
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 WebSphere MQ.

Přesunout správce front do úložiště MSCS

`hamvmqm.exe`

Viz “Přesun správce front do úložiště MSCS” na stránce 321.

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 IBM WebSphere MQ Explorer k jeho odstranění na uzlu, kde momentálně 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

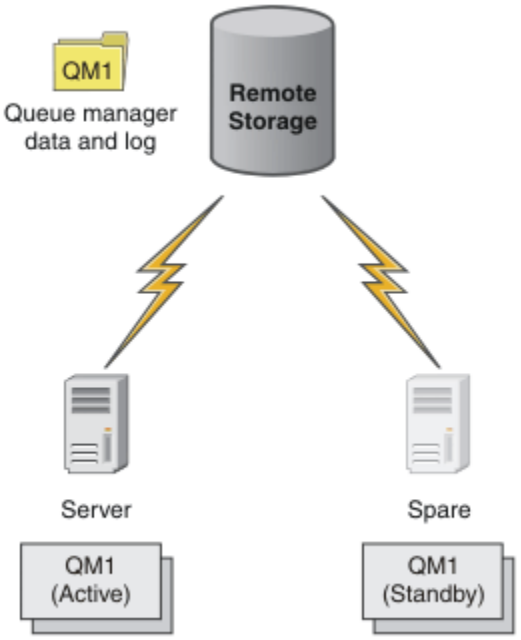
`amqmsysn.exe`

Tento obslužný program zobrazí dialogové okno s úplnými podrobnostmi o nastavení podpory MSCS (IBM WebSphere MQ MSCS), jako je například podpora při volání podpory 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.

Obrázek 63 na stránce 334 zobrazuje konfiguraci s více instancemi pro QM1. Produkt IBM WebSphere 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 63. 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.
- Nereakce na procesy správce front zjištěné produktem WebSphere MQ, která poté ukončí 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.

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 k přenosu připojení produktu WebSphere MQ 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 frontami produktu WebSphere 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.

Klienti a kanály produktu WebSphere MQ MQI 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. Třídy IBM WebSphere MQ pro jazyk Java automatické opětovné připojování klientů nepodporují.

podporované platformy

Správce front pro více instancí můžete vytvořit na libovolném z platforem jiných nežz/OS z verze 7.0.1.

Automatické opětovné připojení klienta je podporováno pro klienty MQI od verze 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 WebSphere MQ na jiném serveru. Správci front s více instancemi sdílená 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 UNIX and Linux . Kroky jsou následující:

1. Vytvořte sdílené prostředky pro data a soubory protokolu.
2. Vytvořte správce front na jednom serveru.
3. Spuštěním příkazu **dspmqinf** na prvním serveru shromážděte konfigurační data správce front a zkopírujte 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.

Na systémech UNIX and Linuxmusíte ve všech systémech učinit `uid` a `gid` `mqm` stejné. Možná budete muset upravit `/etc/passwd` na každém systému, abyste nastavili obecné `uid` a `gid` pro `mqm`, a pak znovu zaveďte systém.

V systému Microsoft Windowsmusí 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 “Zabezpečit data správce sdílených front a adresáře a soubory protokolu v systému Windows” na stránce 361. 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 338demonstruje, 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 352demonstruje, 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 WebSphere MQ na každém serveru. Každý server musí mít nainstalovanou stejnou verzi operačního systému IBM WebSphere MQ na kompatibilní úrovni oprav. Příkazy, **dspmqinf** 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 373, “Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény” na stránce 338a “Vytvoření správce front s více instancemi na řadičích domény” na stránce 352 představují příklady konfigurace správce front pro více instancí.

Na systémech Windows, UNIX and 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 tuto proměnnou.

Omezení

1. Konfigurovat více instancí stejného správce front pouze na serverech se stejným operačním systémem, architekturou a endiannerem. Oba stroje musí být například buď 32bitové, nebo 64bitové.
2. Všechny instalace produktu IBM WebSphere 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 úrovně 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 WebSphere MQ , skupinou a mechanismem řízení přístupu.
5. V systémech UNIX and 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 přerušen systémovým voláním. Měkká připojení nezaručujte 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 Windowsmusí být k síťovému úložišti přistupovat prostřednictvím protokolu CIFS (Common Internet File System) používaného sítěmi Windows .

Windows domén a správců front s více instancemi
Správce front s více instancemi v produktu Windows vyžaduje, aby byly jeho data a protokoly sdíleny. 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.

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 364 a “Zabezpečit data správce sdílených front a adresáře a soubory protokolu v systému Windows” na stránce 361 , abyste přezkoumali, jak řídit přístup k datům správce front a protokolových souborů. Témata jsou vzdělávací; chcete-li přejít přímo na 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 338.

Spustit správce front s více instancemi na pracovních stanicích nebo na serverech domény

V produktu Version 7.1jsou správci front s více instancemi spouštěny na pracovní stanici nebo na serveru, který je členem domény. Před Version 7.1se správci front pro více instancí spouštěli pouze na řadičích domény; viz “Spustit správce front s více instancemi na řadičích domény” na stránce 338. 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 Version 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 338.

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 364. Toto téma obsahuje dvě úlohy, které vám pomohou porozumět krokům, které je třeba provést. Úlohy jsou “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 366 a “Čtení a zápis dat a souborů protokolu autorizovaných alternativní lokální skupinou zabezpečení” na stránce 369. Další téma, “Zabezpečit data správce sdílených front a adresáře a soubory protokolu v systému Windows” na stránce 361, 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 WebSphere MQ for Windowsa konfigurování správce front pro použití sdílení. Úlohy jsou následující:

1. “Vytvoření Active Directory a domény DNS pro IBM WebSphere MQ” na stránce 341.
2. “Instalace produktu IBM WebSphere MQ na server nebo pracovní stanici v doméně Windows” na stránce 344.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu” na stránce 347.
4. “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 349.

Potom můžete provést úlohu “Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény” na stránce 338pomocí 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 Version 7.0.1běžely správci front více instancí pouze na řadičích domény. Data správce front by mohla být zabezpečena pomocí skupiny domén `mqm` . Jak se vysvětluje téma “Zabezpečit data správce sdílených front a adresáře a soubory protokolu v systému Windows” na stránce 361 , 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 WebSphere MQ for Windows na řadiči 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 352 a nakonfigurujte správce front s více instancemi na řadičích domény.

Související informace

uzly klastru Windows 2000, Windows Server 2003 a Windows Server 2008 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 WebSphere MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Server Windows Server 2008 používaný jako druhý server IBM WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

V systému Windowsnení nutné ověřovat systém souborů, do kterého chcete ukládat data správce front a soubory žurnálu. Procedura kontroly, Ověření chování sdíleného systému souborů , je použitelná pro produkt UNIX and Linux. V systému Windowsjsou kontroly vždy úspěšné.

Postupujte podle kroků uvedených v následujících úlohách. Úlohy vytvářejí řadič domény a doménu, instalují produkt IBM WebSphere MQ for Windows na jeden server a vytvářejí sdílení souboru pro data a soubory protokolů. Pokud konfigurujete 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 WebSphere MQ” na stránce 341.
2. “Instalace produktu IBM WebSphere MQ na server nebo pracovní stanici v doméně Windows” na stránce 344.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu” na stránce 347.
4. “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 349.

Informace o této úloze

Tato úloha je jednou z posloupností úloh pro konfiguraci řadiče domény a dvou serverů v doméně za účelem spouštění 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 WebSphere MQ for Windows.
   a) Chcete-li vytvořit druhý server domény, proveďte kroky v úloze “Instalace produktu IBM WebSphere MQ na server nebo pracovní stanici v doméně Windows” na stránce 344 . V této posloupnosti úloh se druhý server nazývá *venus*.

   Tip: Vytvořte druhou instalaci s použitím stejných výchozích nastavení instalace pro produkt IBM WebSphere MQ na každém ze dvou serverů. Pokud se výchozí hodnoty liší, možná budete muset upravit proměnné Předpona a InstallationName ve stanze *QMGR* **QueueManager** v konfiguračním souboru IBM WebSphere 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 349a vytvořte ji.
   b) Zkontrolujte hodnoty parametrů Předpona a InstallationName , které jsou správné pro produkt *venus*.

   V systému *mars*spusťte příkaz **dspmqinf** :

   ```
   dspmqinf QMGR
   ```

   Odezva systému:

   ```
   QueueManager:
      Name=QMGR
      Directory=QMGR
      Prefix=C:\Program Files\IBM\WebSphere MQ
      DataPath=\\sun\wmq\data\QMGR
      InstallationName=Installation1
   ```

   c) Okopírujte strojově čitelnou formu stanzy **QueueManager** do schránky.

   V systému *mars* 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:\Program Files\IBM\WebSphere 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:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

```
WebSphere MQ configuration information added.
```

3. Spusťte správce front *QMGR* v systému *venus*a povolit instance v pohotovostním režimu.
   a) Kontrola *QMGR* na *mars* je zastavena.

   V systému *mars*spusťte příkaz **dspmq** :

   ```
   dspmq -m QMGR
   ```

   Odezva systému závisí na tom, jak byl správce front zastaven; například:

   ```
   C:\Users\Administrator>dspmq -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:

   ```
   WebSphere 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'.
   WebSphere 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 standbys:

   ```
   strmqm -x QMGR
   ```

   Odezva systému:

   ```
   WebSphere 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*:

   ```
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ended, permitting switchover to
   a standby instance.
   ```

A v systému *mars*:

```
dspmq
QMNAME(QMGR) STATUS(Running as standby)
C:\Users\wmquser2>dspmq
QMNAME(QMGR) STATUS(Running as standby)
C:\Users\wmquser2>dspmq
QMNAME(QMGR)  STATUS(Running)
```

Jak pokračovat dále

Chcete-li ověřit správce front s více instancemi pomocí ukázkových programů, přečtěte si téma “Ověření správce front pro více instancí v systému Windows” na stránce 359.

Vytvoření Active Directory a domény DNS pro IBM WebSphere 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 WebSphere MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
: Server Windows Server 2008 používaný jako druhý server IBM WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Kroky úlohy jsou konzistentní se serverem Windows Server 2008, který je nainstalován, ale není nakonfigurován s žádnou rolí. Pokud konfigurujete 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 nakonfigurujete tak, aby byl připraven k instalaci produktu IBM WebSphere MQ na jiných serverech a pracovních stanicích, které se připojí k doméně. Pokud nejste obeznámeni s instalací a konfigurací produktu Active Directory , abyste vytvořili doménu 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 sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu "Windows domén a správců front s více instancemi" na stránce 336.

Pro účely úlohy je název hostitele řadiče domény *sun*a tyto dva servery IBM WebSphere 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 `dcpromo` a klepněte na **OK**.

   Nejsou-li binární soubory Active Directory již nainstalovány, produkt Windows automaticky nainstaluje soubory.
3. V prvním okně průvodce ponechte zaškrtávací 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 , který je podporován produktem IBM WebSphere 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 Forest na **Windows Server 2003**.
7. Otevře se okno Další volby řadiče domény s volbou **Server DNS** jako přídavnou 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*\`Adminstrator`.

    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 WebSphere MQ" na pracovní stanici nebo serveru domény. Způsobí to, že "Průvodce přípravou produktu IBM WebSphere MQ" automaticky přidá skupinu `Domain mqm` do lokální skupiny `mqm` v každé nové instalaci produktu IBM WebSphere MQ v dané doméně.
    - Pracovní stanice nebo servery v doméně můžete instalovat 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 WebSphere 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. Jednotlivé skupiny domén přidejte do lokální skupiny mqm v různých instalacích produktu IBM WebSphere 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 WebSphere 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 Číst členství ve skupině** a **Povolit Číst groupMembershipSAM** , která se bude používat pro globální skupinu Domain mqm .
    a) V řádku 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 **Použít na** vyberte ze spodní části seznamu volbu **Podřízené objekty uživatele**.
    f) V seznamu **Oprávnění** vyberte zaškrtávací políčka **Číst členství ve skupině** a **Číst groupMembershipSAM Povolit** . Klepněte na tlačítko **OK** > **Použít** > **OK** > **OK**.
14. Přidejte dva nebo více uživatelů do globální skupiny Domain mqm .

    Jeden uživatel, *wmquser1* v příkladu, spouští službu IBM IBM WebSphere 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 WebSphere MQ" automaticky nakonfiguruje produkt Domain mqm jako člena lokální skupiny mqm , kde je průvodce spuštěn.
    Chcete-li spustit službu IBM IBM WebSphere MQ pro každou instalaci produktu IBM WebSphere MQ na jednom počítači, musíte zadat jiného uživatele. Stejné uživatele můžete znovu použít na různých počítačích.

    a) Ve stromu navigace správce serveru klepněte na nabídku **Uživatelé** > **Nový** > **Uživatel** .
    b) 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**.
    c) Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a zrušte označení zaškrtávacího políčka **Uživatel musí změnit heslo při příštím přihlášení** . Klepněte na tlačítko **Další** > **Dokončit**.
    d) V okně Users klepněte pravým tlačítkem myši na ***WebSphere MQ*** > **Přidat do skupiny ...**. Zadejte Domain mqm a klepněte na **Zkontrolovat názvy** > **OK** > **OK**.
    e) Opakujte kroky a až d , chcete-li přidat *WebSphere MQ2* jako *wmquser2*.
15. Spuštění IBM WebSphere MQ jako služby.

    Pokud potřebujete spustit produkt IBM WebSphere MQ jako službu a poté poskytnout uživateli domény (který jste získali od administrátora domény) právo spouštět jako službu, proveďte následující postup:

a) Klepněte na tlačítko **Start > Spustit ...**.

   Zadejte příkaz `secpol.msc` a klepněte na tlačítko **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 ...**

   Zadejte jméno uživatele, kterého jste získali od administrátora domény, a klepněte na **Kontrolovat názvy** .

d) Pokud jste vyzváni oknem Zabezpečení produktu Windows , zadejte jméno uživatele a heslo účtu uživatele nebo administrátora s dostatečným oprávněním a klepněte na tlačítko **OK > Použít > OK**.

   Zavřete okno Lokální zásada zabezpečení.

Poznámka: Na systémech Windows Vista a Windows Server 2008 je služba UAC (User Account Control) povolena při výchozím nastavení.

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 WebSphere MQ na server nebo pracovní stanici v doméně Windows" na stránce 344.

Instalace produktu IBM WebSphere MQ na server nebo pracovní stanici v doméně Windows
V této úloze nainstalujete a nakonfigurujete produkt IBM WebSphere 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 WebSphere MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Server Windows Server 2008 používaný jako druhý server IBM WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte 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 WebSphere MQ" na stránce 341 . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
2. Další verze produktu Windows , na kterých můžete produkt IBM WebSphere MQ spustit, najdete v tématu Hardwarové a softwarové požadavky na systémech Windows .

Informace o této úloze

V této úloze nakonfigurujete produkt Windows Server 2008 s názvem *mars*jako člen domény *wmq.example.com* . Nainstalujte produkt IBM WebSphere MQa nakonfigurujte instalaci tak, aby se spouštěla jako člen domény *wmq.example.com* .

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 336.

Pro účely úlohy je název hostitele řadiče domény *sun*a tyto dva servery IBM WebSphere 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**.

      Systém 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 zkontrolli 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 WebSphere MQ for Windows na *mars*.

   Další informace o spouštění průvodce instalací produktu IBM WebSphere MQ for Windows naleznete v tématu Instalace serveru IBM WebSphere MQ v systému Windows .

a) V systému *mars*se přihlaste jako lokální administrátor, *mars*\Administrator.

b) Spusťte příkaz **Setup** na instalačním médiu produktu IBM WebSphere MQ for Windows .

Spustí se příruční panel produktu IBM WebSphere 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 WebSphere MQ" na stránce 341, konfiguruje ID uživatele domény pro tuto sadu úloh.

e) Klepněte na volbu **Instalace produktuWebSphere MQ**, vyberte jazyk instalace a klepněte na volbu Spustit instalační program produktu IBM IBM WebSphere 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**.

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 WebSphere MQ je instalován a instalační program spustí "Průvodce přípravou produktu IBM WebSphere MQ" .

Důležité: Ještě nespouštějte průvodce.

5. Nakonfigurujte uživatele, který bude spouštět službu IBM IBM WebSphere MQ s právem **Spustit jako služba** .

Vyberte, zda chcete konfigurovat lokální skupinu mqm , skupinu Domain mqm nebo uživatele, který bude spouštět službu IBM IBM WebSphere 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 volbu **Přihlášení 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*\Administratora klepněte na tlačítko **OK** > **Použít** > **OK**. Zavřete okno Lokální zásada zabezpečení.

6. Spusťte průvodce "Příprava produktu IBM WebSphere MQ" .

Další informace o spuštění průvodce "Prepare IBM WebSphere MQ" naleznete v tématu Konfigurace produktu WebSphere MQ s pomocí Průvodce přípravou produktu WebSphere MQ .

a) Instalační program produktu IBM IBM WebSphere MQ automaticky spustí "Příprava produktu IBM WebSphere MQ" .

Chcete-li spustit průvodce ručně, vyhledejte zástupce "Připravit IBM WebSphere MQ" ve složce **Start** > **Všechny programy** > **IBM WebSphere MQ** . Vyberte zástupce, který odpovídá instalaci produktu IBM WebSphere 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 prvním okně Konfigurace produktu IBM WebSphere MQ for Windows pro doménu uživatelů produktu Windows .

d) V druhém okně Konfigurace produktu IBM WebSphere MQ for Windows pro uživatele domény produktu Windows zadejte do pole **Doména** hodnotu *wmq* . Zadejte *wmquser1* do pole **Jméno uživatele** a heslo, pokud jste jej nastavili, v poli **Heslo** . Klepněte na tlačítko **Další**.

Průvodce nakonfiguruje a spustí IBM IBM WebSphere MQ s *wmquser1*.

e) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí zaškrtávacích políček podle potřeby a klepněte na tlačítko **Dokončit**.

Jak pokračovat dále

1. Proveďte úlohu “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 366, abyste ověřili, že instalace a konfigurace fungují správně.
2. Proveďte úlohu “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu” na stránce 347, chcete-li konfigurovat sdílení souborů pro ukládání dat a souborů protokolu správce front s více instancemi.

Související pojmy

Uživatelská práva vyžadovaná pro službu systému Windows produktu WebSphere MQ

Vytvoření sdíleného adresáře pro data správce front a soubory protokolu

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle 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 WebSphere MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
: Server Windows Server 2008 používaný jako druhý server IBM WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li provést tuto úlohu přesně tak, jak je zdokumentováno, proveďte kroky v úloze “Vytvoření Active Directory a domény DNS pro IBM WebSphere MQ” na stránce 341, abyste vytvořili 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 sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 336.

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 WebSphere 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 WebSphere MQ . Proto jsou *wmquser1* a *wmquser2* členy lokální skupiny mqm na obou serverechIBM WebSphere 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 *wmquser1* a *wmquser2* 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 *wmquser1; wmquser2* 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 zaškrtávacího políčka **Zahrnout oprávnění k dědičné oprávnění u vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení systému 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 zaškrtávací 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 zaškrtávací políčko **Úplné řízení** v seznamu **Oprávnění pro *wmqha***; klepněte na tlačítko **Použít**.

l) Vyberte položku *Administrators* v seznamu **Názvy skupin nebo uživatelů**. Vyberte zaškrtávací políčko **Úplné řízení** v seznamu **Oprávnění pro *Administrátoři***; klepněte na nabídku **Použít** > **OK** > **OK** > **Zavřít**.

Jak pokračovat dále

Zkontrolujte, zda je možné číst a zapisovat soubory do sdílených adresářů z každého ze serverů IBM WebSphere MQ . Zkontrolujte ID uživatele služby IBM IBM WebSphere MQ , *wmquser1* a interaktivní ID uživatele *wmquser2*.

1. Používáte-li vzdálenou pracovní plochu, musíte přidat *wmq**wmquser1* a *wmquser2* 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 *wmquser1*; *wmquser2* 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*.

      Systém 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 349.

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 protokorovým 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 WebSphere MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Server Windows Server 2008 používaný jako druhý server IBM WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

Postupujte podle kroků uvedených v následujících úlohách. Úlohy vytvářejí řadič domény a doménu, instalují produkt IBM WebSphere MQ for Windows na jeden server a vytvářejí sdílení souboru pro data a soubory protokolů. Pokud konfigurujete 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 WebSphere MQ” na stránce 341.
2. “Instalace produktu IBM WebSphere MQ na server nebo pracovní stanici v doméně Windows” na stránce 344.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu” na stránce 347.

Informace o této úloze

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 336.

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 IBM WebSphere MQ .

   Službu musíte restartovat, aby ID uživatele, pod kterým je spuštěna, získalo další pověření zabezpečení, která jste pro ni nakonfigurovali.

   Zadejte příkazy:

   ```
   endmqsvc
   strmqsvc
   ```

   Odezvy systému:

   ```
   5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
   The MQ service for installation 'Installation1' ended successfully.
   A:
   5724-H72 (C) Copyright IBM Corp. 1994, 2024. 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:

   ```
   WebSphere 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 vložením a získáním zprávy do fronty.

1. Spusťte správce front.

   ```
   strmqm QMGR
   ```

   Odezva systému:

   ```
   WebSphere 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'.
   WebSphere 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, 2024. ALL RIGHTS RESERVED.
   Starting MQSC for queue manager QMGR.


        1 : define qlocal(QTEST)
   AMQ8006: WebSphere 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:

```
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

```
WebSphere MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

Tip: Přidejte volbu `/Q` k příkazům, abyste zabránili náznaku příkazu k odstranění každého souboru nebo adresáře.

```
del /F /S C:\wmq\*.*
rmdir /S C:\wmq
```

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 338.

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 WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

mars
Server Windows Server 2008 používaný jako souborový server.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. V systému Windowsnení nutné ověřovat systém souborů, do kterého chcete ukládat data správce front a soubory žurnálu. Procedura kontroly, Ověření chování sdíleného systému souborů , je použitelná pro produkt UNIX and Linux. V systému Windowsjsou kontroly vždy úspěšné.
2. Chcete-li vytvořit první řadič domény, proveďte kroky v části “Vytvoření Active Directory a domény DNS pro IBM WebSphere MQ” na stránce 341 .
3. Chcete-li přidat druhý řadič domény, nainstalujte produkt IBM WebSphere 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 355 .
4. Proveďte kroky uvedené v části “Instalace produktu IBM WebSphere MQ na řadičích domény v doméně wmq.example.com” na stránce 357 a nainstalujte produkt IBM WebSphere 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 zaškrtávacího políčka **Zahrnout oprávnění k dědičné oprávnění u vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení systému 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 systému Windows zadejte jméno 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 zaškrtávací 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 systému Windows zadejte jméno 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:

   ```
   WebSphere 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:

```
WebSphere 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'.
WebSphere 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:\Program Files\IBM\WebSphere 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:\Program Files\IBM\WebSphere 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
```

```
WebSphere MQ configuration information added.
```

6. Spusťte instanci v pohotovostním režimu správce front v systému *earth*.

```
strmqm -x QMGR
```

Odezva systému:

```
WebSphere 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*:

   ```
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere 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 “Ověření správce front pro více instancí v systému Windows” na stránce 359.

Související úlohy

“Přidání druhého řadiče domény do domény wmq.example.com” na stránce 355

“Instalace produktu IBM WebSphere MQ na řadičích domény v doméně wmq.example.com” na stránce 357

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 WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

mars
: Server Windows Server 2008 používaný jako souborový server.

Nahraďte 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 WebSphere MQ” na stránce 341 . 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 sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 336.

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**.

      Systém 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 zkontrolli 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 automaticky nainstaluje soubory.
4. Konfigurujte *earth* jako druhý řadič domény v doméně *wmq.example.com* .
   a) V prvním okně průvodce ponechte zaškrtávací 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 WebSphere MQ; viz “Instalace produktu IBM WebSphere MQ na řadičích domény v doméně wmq.example.com” na stránce 357.

Související úlohy

“Vytvoření Active Directory a domény DNS pro IBM WebSphere MQ” na stránce 341

Instalace produktu IBM WebSphere MQ na řadičích domény v doméně wmq.example.com
Nainstalujte a nakonfigurujte instalace produktu IBM WebSphere MQ na obou řadičích domény v doméně *wmq.example.com* .
Sem zadejte krátký popis; použije 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 WebSphere MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

mars
Server Windows Server 2008 používaný jako souborový server.

Nahraďte 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 WebSphere MQ” na stránce 341 . 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 355 . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
3. Další verze produktu Windows , na kterých můžete spustit produkt IBM WebSphere MQ , najdete v tématu Hardwarové a softwarové požadavky na systémech Windows .

Informace o této úloze

Nainstalujte a nakonfigurujte instalace produktu IBM WebSphere MQ na obou řadičích domény v doméně *wmq.example.com* .

Postup

1. Nainstalujte IBM WebSphere MQ na *sun* a *earth*.

   Další informace o spouštění průvodce instalací produktu IBM WebSphere MQ for Windows naleznete v tématu Instalace serveru IBM WebSphere 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 WebSphere MQ for Windows .

      Spustí se příruční panel produktu IBM WebSphere 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 **Instalace produktuWebSphere MQ**, vyberte jazyk instalace a klepněte na volbu Spustit instalační program produktu IBM IBM WebSphere 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 WebSphere MQ je instalován a instalační program spustí průvodce "Příprava produktu IBM WebSphere MQ" .

   Instalace produktu IBM WebSphere MQ for Windows nakonfiguruje lokální skupinu domén `mqm`a skupinu domén `Domain mqm`. `Domain mqm` je členem `mqm`. Následné řadiče domény ve stejné doméně sdílejí skupiny `mqm` a `Domain mqm` .

2. V produktu *earth* i v produktu *sun*spusťte "Průvodce přípravou produktu IBM WebSphere MQ" .

   Další informace o spuštění průvodce "Prepare IBM WebSphere MQ" naleznete v tématu Konfigurace produktu WebSphere MQ pomocí Průvodce přípravou produktu WebSphere MQ .

   a) Instalační program produktu IBM WebSphere MQ spustí automaticky "Příprava produktu IBM WebSphere MQ" .

      Chcete-li spustit průvodce ručně, vyhledejte zástupce "Připravit IBM WebSphere MQ" ve složce **Start** > **Všechny programy** > **IBM WebSphere MQ** . Vyberte zástupce, který odpovídá instalaci produktu IBM WebSphere 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 **Ne** .[1].

   c) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí zaškrtávacích políček podle potřeby a klepněte na tlačítko **Dokončit**.

   Průvodce "Příprava produktu IBM WebSphere 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 IBM WebSphere MQ na každém řadiči, s `MUSR_MQADMIN` nebo `MUSR_MQADMIN1` jako uživatele, který se přihlásí na službu.

[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 WebSphere MQ , jako by se nenachází v doméně.

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 zadejte `mqm`; klepněte na **Zkontrolovat názvy** > **OK** > **OK**

Výsledky

1. Zkontrolujte, zda "Prepare IBM WebSphere 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 ...** > **Člen**a uvidíte, že se jedná o člena `Domain users` a `mqm`.

2. Zkontrolujte, že produkt `MUSR_MQADMIN` má právo pracovat jako služba:

   a. Klepněte naKlepněte 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 volbu **Přihlášení jako služba** > **Vlastnosti**a viz `MUSR_MQADMIN` se uvádí jako mající právo přihlásit se jako služba. Klepněte na tlačítko **OK**.

Jak pokračovat dále

1. Proveďte úlohu “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 366, abyste ověřili, že instalace a konfigurace fungují správně.
2. Přejděte zpět na úlohu “Vytvoření správce front s více instancemi na řadičích domény” na stránce 352, abyste dokončili úlohu konfigurace správce front s více instancemi na řadičích domény.

Související pojmy

Uživatelská práva vyžadovaná pro službu systému Windows produktu WebSphere MQ

Ověření správce front pro více instancí v systému Windows

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 na systému 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 352. 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 o velikosti 400 MB VMware se systémem Windows XP s aktualizací Service Pack 2. 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 produktu WebSphere MQ

Než použijete ukázkové aplikace k ověření překonání selhání, spusťte na každém serveru produkt WebSphere MQ Explorer. 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) +
       CONNAME('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)
```

   Případně můžete použít Průzkumníka WebSphere MQ Explorer, který je spuštěn modulem 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. Proveďte jednu z následujících akcí:
   - Zavřete okno se spuštěnou instancí serveru VMware s obrazem aktivního serveru.
   - Pomocí Průzkumníka produktu WebSphere MQ zastavte aktivní instanci správce front, což umožňuje přepnutí na záložní instanci a instruování opakovaného připojení klientů 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 všechna tři spojení znovu zavedne. 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:\>amqsghac 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>
```

Zabezpečit data správce sdílených front a adresáře a soubory protokolu 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 WebSphere MQ for Windows, instalační program vytvoří domovský adresář dle vašeho výběru pro

všechny správce front, kteří jsou na tomto serveru vytvoři. Zazabezpečuje adresáře s lokální skupinou mqm a konfiguruje ID uživatele pro službu IBM IBM WebSphere 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.

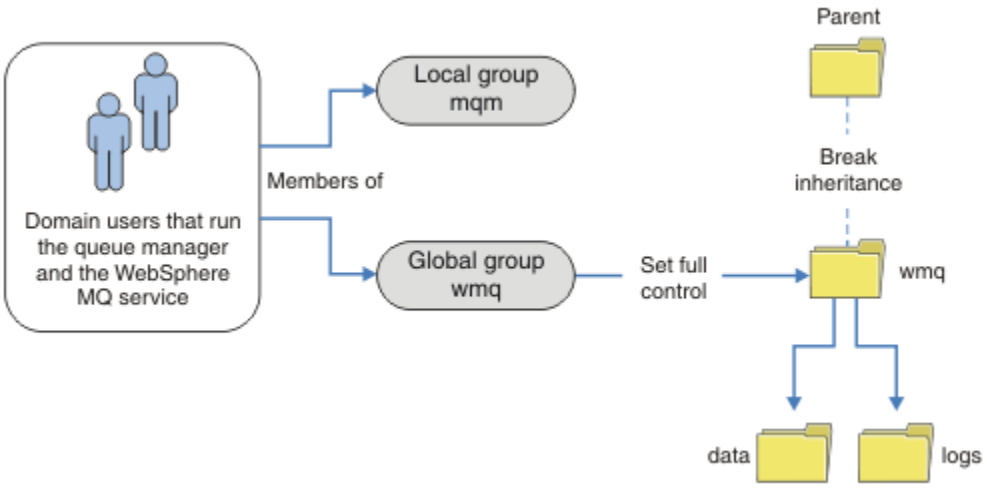
Zadání správce front s globální alternativní skupinou zabezpečení tento problém řeší; viz Obrázek 64 na stránce 362 . Zabezpečte vzdálenou složku s globální skupinou. Když jej vytvoříte v systému *mars*, předejte název globální skupiny ke správci front. Předejte název globální skupiny jako alternativní 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 stanze **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 truea byla poskytnuta také skupina přístupů, lokální skupina mqm nemá udělen přístup k datovým souborům správce front.

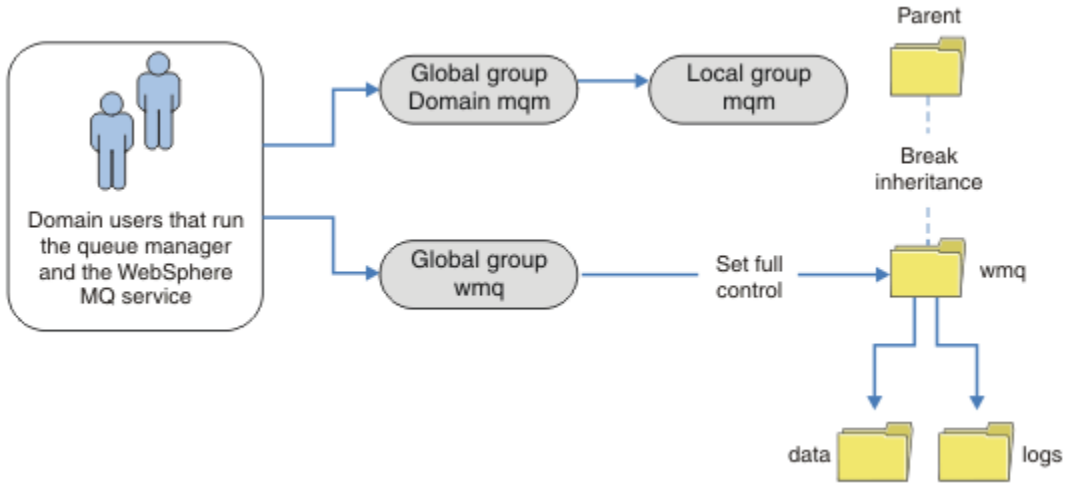


Obrázek 64. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (1)

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 64 na stránce 362 se uživatelům, kteří spouštějí procesy správce front, zobrazují jako uživatelé domény.

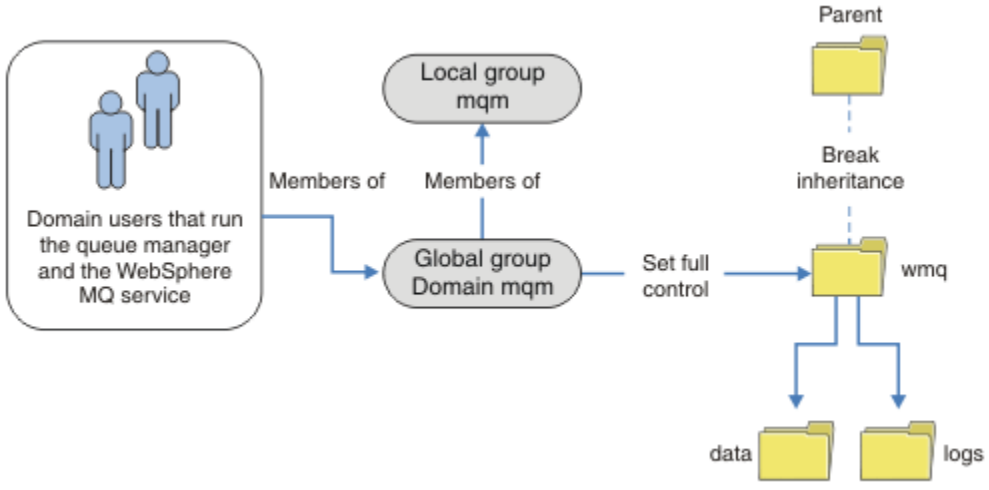
Pokud implementujete mnoho serverů IBM WebSphere MQ , seskupování uživatelů v produktu Obrázek 64 na stránce 362 není vhodné. Budete muset opakovat proces přidání uživatelů do lokálních skupin pro každý server IBM WebSphere MQ . Místo toho vytvořte na řadiči domény globální skupinu `Domain mqm` a vytvořte uživatele, kteří spouštějí členy IBM WebSphere MQ skupiny `Domain mqm` ; viz Obrázek 65 na stránce 363 . Když instalujete produkt IBM WebSphere MQ jako instalaci domény, průvodce "Prepare IBM WebSphere MQ" automaticky nastaví skupinu `Domain mqm` jako člena lokální skupiny `mqm` . Tytéž uživatelé jsou v obou globálních skupinách `Domain mqm` a `wmq`.

Tip: Stejní uživatelé mohou spouštět produkt IBM WebSphere MQ na různých serverech, ale na individuálním serveru musíte mít různé uživatele ke spuštění produktu IBM WebSphere 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.



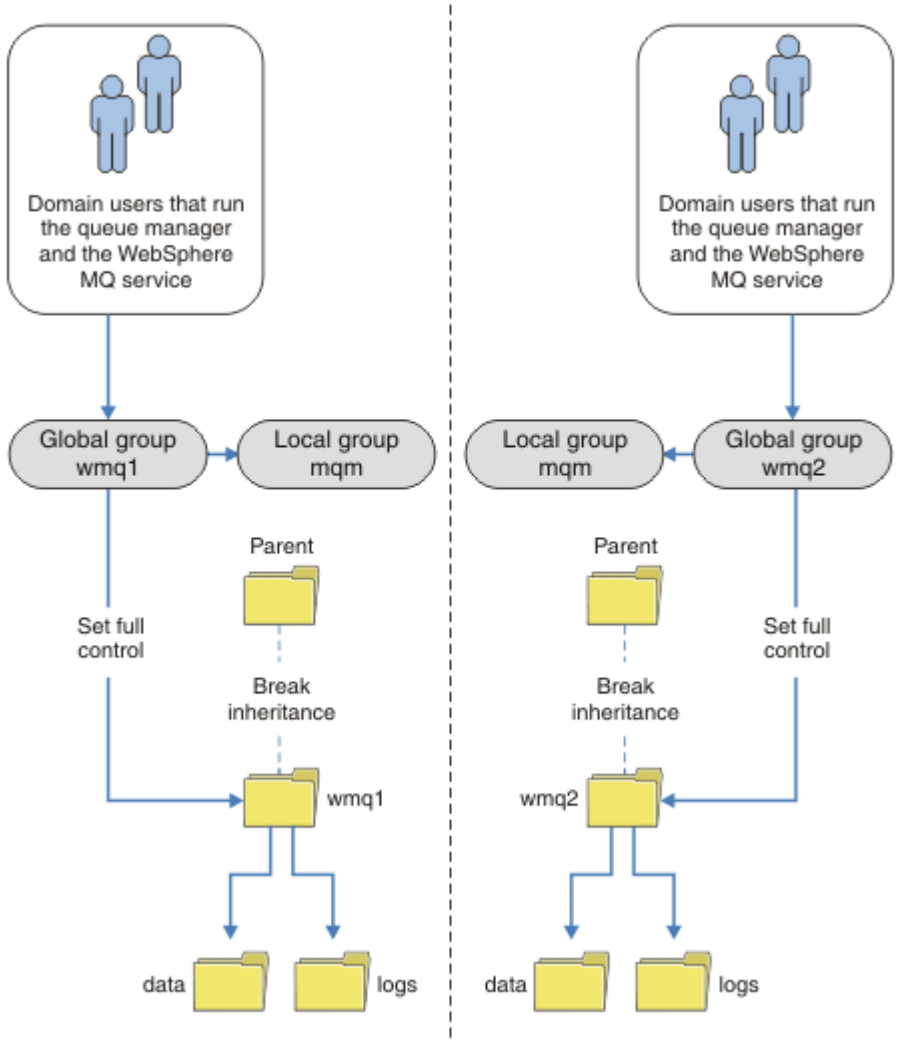
Obrázek 65. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (2)

Organizace v produktu Obrázek 65 na stránce 363 je zbytečně komplikovaná, jak stojí. Uspořádání má dvě globální skupiny se shodnými členy. Můžete zjednodušit organizaci a definovat pouze jednu globální skupinu; viz Obrázek 66 na stránce 363.



Obrázek 66. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (3)

Případně můžete potřebovat podrobnější úroveň řízení přístupu, kdy různí správci front omezeni na přístup k různým složkám. Další informace viz Obrázek 67 na stránce 364. V produktu Obrázek 67 na stránce 364jsou definovány dvě skupiny uživatelů domény, v samostatných globálních skupinách pro zabezpečení různých protokolů správce front a datových souborů. Jsou zobrazeny dvě různé lokální skupiny `mqm` , které musí být na různých serverech IBM WebSphere 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 WebSphere MQ šíří `Domain mqm` do lokální skupiny `mqm` jako v Obrázek 66 na stránce 363, protože existují dvě skupiny uživatelů.



Obrázek 67. 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 66 na stránce 363.

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 WebSphere MQ for Windows, instalační program vytvoří domovský adresář dle vašeho výběru pro všechny správce front, které jsou vytvořeny. Zazabezpečuje adresáře s lokální skupinou `mqm` a konfiguruje ID uživatele pro službu IBM IBM WebSphere MQ pro přístup k adresářům.

Dva příklady demonstrují, jak nakonfigurovat řízení přístupu pro produkt IBM WebSphere 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 autorizovaných lokální skupinou mqm” na stránce 366, povolíte přístup k adresářům a adresářům protokolu tím, že udělíte oprávnění od lokální skupiny `mqm` . Druhý příklad, “Čtení a zápis dat a souborů protokolu autorizovaných alternativní lokální skupinou zabezpečení” na stránce 369, 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. Pokud k adresářům přistupuje správce front spuštěnému na různých serverech, jako například správce front s více instancemi, zabezpečení dat a souborů protokolu s alternativní skupinou zabezpečení je jedinou volbou. Další informace naleznete v tématu “Zabezpečit data správce sdílených front a adresáře a soubory protokolu v systému Windows” na stránce 361.

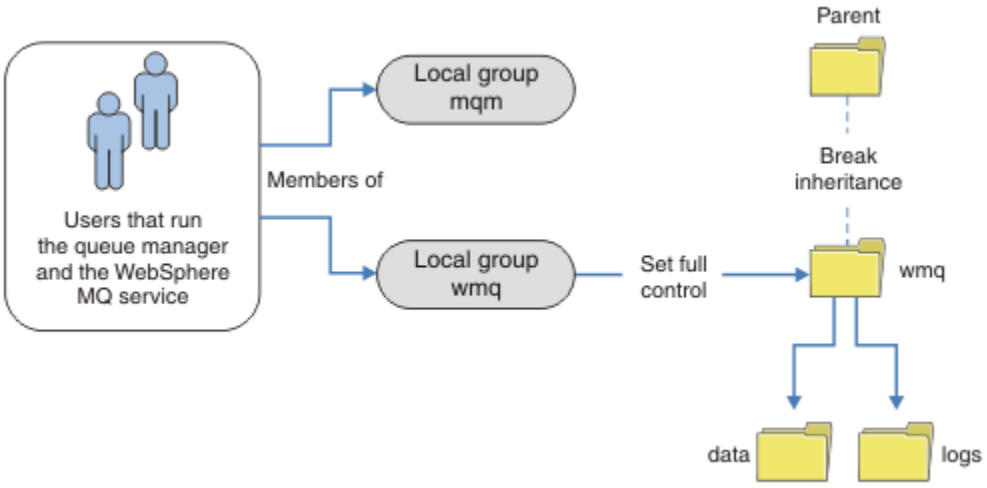
Konfigurace oprávnění zabezpečení dat správce front a souborů protokolu není běžná úloha v produktu Windows. Když instalujete produkt IBM WebSphere MQ for Windows, buď zadejte adresáře pro data a protokoly správce front, nebo přijměte výchozí adresáře. Instalační program automaticky zabezpečuje tyto 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 nadřízené 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 WebSphere MQ , musí být toto ID uživatele členem lokální skupiny `mqm` . Úloha “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 366vás 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 68 na stránce 366. Jako příklad alternativní skupiny zabezpečení je použita lokální skupina `wmq`.



Obrázek 68. 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 nadřízený adresář.
2. Zkopírujte existující sadu zděděných oprávnění pro adresáře nebo nadřízený 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 “Zabezpečit data správce sdílených front a adresáře a soubory protokolu v systému Windows” na stránce 361.
5. Vytvořte správce front s uvedením alternativní skupiny zabezpečení nebo činitele v příkazu **`crtmqm`** s parametrem `-a` .

Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm
Tato úloha ilustruje, jak vytvořit správce front s jeho daty a soubory protokolů uloženými v libovolném adresáři podle vaší volby. Přístup k souborům je zabezpečen lokální skupinou `mqm` . Adresář není sdílený.

Než začnete

1. Nainstalujte produkt IBM WebSphere MQ for Windows jako primární instalaci.
2. Spusťte průvodce "Připravit IBM WebSphere MQ" . Pro tuto úlohu nakonfigurujte instalaci tak, aby byla spuštěna buď s ID lokálního uživatele, nebo s ID uživatele domény. Nakonec, chcete-li dokončit všechny úlohy v produktu “Windows domén a správců front s více instancemi” na stránce 336, musí být instalace nakonfigurována pro doménu.
3. Chcete-li provést první část úlohy, přihlaste se s oprávněním administrátora.

Informace o této úloze

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 336.

V systému Windowsmůžete vytvořit výchozí cesty k datům a protokolům pro server IBM WebSphere MQ for Windows v libovolném adresáři dle vaší volby. Průvodce instalací a konfigurací automaticky poskytne lokální skupině `mqm` a ID uživatele, který spouští procesy správce front, přístup k adresářům. Pokud vytvoříte správce front s určením různých adresářů pro data správce front a soubory protokolu, musíte nakonfigurovat oprávnění k úplnému řízení adresářů.

V tomto příkladu udělíte správci front úplnou kontrolu nad jeho daty a soubory protokolu tím, že udělíte lokální skupině `mqm` oprávnění k adresáři *c:\wmq*.

Příkaz **crtmqm** vytvoří správce front, který se automaticky spustí při spuštění pracovní stanice pomocí služby IBM IBM WebSphere MQ .

Úloha je ilustrativní; používá specifické hodnoty, které můžete změnit. Hodnoty, které můžete změnit, jsou kurzívou. Na konci úlohy postupujte podle pokynů a odeberte všechny změny, které jste provedli.

Postup

1. Otevřete příkazový řádek.
2. Zadejte příkaz:

   ```
   md c:\wmq\data , c:\wmq\logs
   ```

3. Nastavte oprávnění k adresářům, abyste povolili 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 pro realistickou produkční konfiguraci pokračujte s ID uživatele s omezenějšími právy. ID uživatele musí být alespoň členem lokální skupiny `mqm` .

   Pokud je instalace produktu IBM WebSphere MQ konfigurována jako součást domény, učiňte ID uživatele členem skupiny `Domain mqm` . Průvodce "Připravit IBM WebSphere MQ" učiní globální skupinu `Domain mqm` členem lokální skupiny `mqm` , takže nemusíte přímo nastavit ID uživatele jako člena 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:

   ```
   WebSphere 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 se adresáře vytvořené správcem front nacházejí v adresáři *c:\wmq* .

```
dir c:\wmq /D /B /S
```

7. Zkontrolujte, zda mají soubory oprávnění ke čtení a zápisu nebo úplné řízení pro lokální skupinu mqm .

```
cacls c:\wmq\*.*
```

Jak pokračovat dále

Otestujte správce front vložením a získáním zprávy do fronty.

1. Spusťte správce front.

```
strmqm QMGR
```

Odezva systému:

```
WebSphere 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'.
WebSphere 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, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QMGR.


     1 : define qlocal(QTEST)
AMQ8006: WebSphere 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:

```
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

```
WebSphere MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

Tip: Přidejte volbu /Q k příkazům, abyste zabránili náznaku příkazu k odstranění každého souboru nebo adresáře.

```
del /F /S C:\wmq\*.*
rmdir /S C:\wmq
```

Související pojmy

“Windows domén a správců front s více instancemi” na stránce 336
Správce front s více instancemi v produktu Windows vyžaduje, aby byly jeho data a protokoly sdíleny. 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 autorizovaných alternativní lokální skupinou zabezpečení” na stránce 369
Tato úloha ukazuje, jak použít příznak -a v příkazu **crtmqm** . Tento příznak poskytuje správci front alternativní lokální skupinu zabezpečení, která mu poskytuje přístup k jeho protokolům a datovým souborům.

“Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 349
“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény” na stránce 338

Čtení a zápis dat a souborů protokolu autorizovaných alternativní lokální skupinou zabezpečení
Tato úloha ukazuje, jak použít příznak -a v příkazu **crtmqm** . Tento příznak poskytuje správci front alternativní lokální skupinu zabezpečení, která mu poskytuje přístup k jeho protokolům a datovým souborům.

Než začnete

1. Nainstalujte produkt IBM WebSphere MQ for Windows jako primární instalaci.
2. Spusťte průvodce "Připravit IBM WebSphere MQ" . Pro tuto úlohu nakonfigurujte instalaci tak, aby byla spuštěna buď s ID lokálního uživatele, nebo s ID uživatele domény. Nakonec, chcete-li dokončit všechny úlohy v produktu “Windows domén a správců front s více instancemi” na stránce 336, musí být instalace nakonfigurována pro doménu.
3. Chcete-li provést první část úlohy, přihlaste se s oprávněním administrátora.

Informace o této úloze

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů

protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu "Windows domén a správců front s více instancemi" na stránce 336.

V systému Windowsmůžete vytvořit výchozí cesty k datům a protokolům pro server IBM WebSphere MQ for Windows v libovolném adresáři dle vaší volby. Průvodce instalací a konfigurací automaticky poskytne lokální skupině `mqm` a ID uživatele, který spouští procesy správce front, přístup k adresářům. Pokud vytvoříte správce front s určením různých adresářů pro data správce front a soubory protokolu, musíte nakonfigurovat oprávnění k úplnému řízení adresářů.

V tomto příkladu poskytnete správci front alternativní lokální skupinu zabezpečení, která má úplnou autorizaci řízení k adresářům. Alternativní skupina zabezpečení uděluje správci front oprávnění ke správě souborů v adresáři. Primárním účelem alternativní skupiny zabezpečení je autorizovat alternativní globální skupinu zabezpečení. Chcete-li nastavit správce front pro více instancí, použijte alternativní globální skupinu zabezpečení. V tomto příkladu nakonfigurujete lokální skupinu, abyste se seznámili s použitím alternativní skupiny zabezpečení bez instalace produktu IBM WebSphere MQ v doméně. Je neobvyklé konfigurovat lokální skupinu jako alternativní skupinu zabezpečení.

Příkaz **`crtmqm`** vytvoří správce front, který se automaticky spustí při spuštění pracovní stanice pomocí služby IBM IBM WebSphere MQ .

Úloha je ilustrativní; používá specifické hodnoty, které můžete změnit. Hodnoty, které můžete změnit, jsou kurzívou. Na konci úlohy postupujte podle pokynů a odeberte všechny změny, které jste provedli.

Postup

1. Nastavte alternativní skupinu zabezpečení.

   Alternativní skupinou zabezpečení je obvykle skupina domény. V tomto příkladu vytvoříte správce front, který používá lokální alternativní skupinu zabezpečení. Pomocí lokální alternativní skupiny zabezpečení můžete provést úlohu s instalací produktu IBM WebSphere MQ , která není součástí domény.

   a) Spuštěním příkazu **`lusrmgr.msc`** otevřete okno Lokální uživatelé a skupiny.

   b) Klepněte pravým tlačítkem myši na volbu **Skupiny** > **Nová skupina ...**

   c) Do pole **Název skupiny** zadejte *`altmqm`* a klepněte na tlačítko **Vytvořit** > **Zavřít**.

   d) Identifikujte ID uživatele, který spouští službu IBM IBM WebSphere MQ .

      i) Klepněte na tlačítko **Spustit** > **Spustit ...**, Zadejte `services.msc` a klepněte na tlačítko **OK**.

      ii) Klepněte na službu IBM IBM WebSphere 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 IBM WebSphere MQ , do skupiny *`altmqm`* . Přidejte také ID uživatele, pod kterým se přihlásíte, abyste vytvořili správce front, a spusťte jej interaktivně.

      Produkt Windows kontroluje oprávnění správce front pro přístup k adresářům dat a protokolů kontrolou oprávnění ID uživatele, který spouští procesy správce front. ID uživatele musí být členem, přímo či nepřímo prostřednictvím globální skupiny, skupiny *`altmqm`* , která autorizovala adresáře.

      Pokud jste nainstalovali produkt IBM WebSphere MQ jako součást domény a chystáte se provést úlohy v produktu "Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény" na stránce 338, ID uživatelů domény vytvořená v "Vytvoření Active Directory a domény DNS pro IBM WebSphere MQ" na stránce 341 jsou *`wmquser1`* a *`wmquser2`*.

      Pokud jste nenainstalovali správce front jako součást domény, výchozí ID lokálního uživatele, který spouští službu IBM IBM WebSphere MQ , je `MUSR_MQADMIN`. Pokud zamýšlíte provést úlohy bez oprávnění administrátora, vytvořte uživatele, který je členem lokální skupiny `mqm` .

      Postupujte takto, chcete-li přidat *`wmquser1`* a *`wmquser2`* do *`altmqm`*. Pokud se vaše konfigurace liší, nahraďte jména ID uživatelů a skupiny.

      i) V seznamu skupin klepněte pravým tlačítkem myši na volbu **altmqm** > **Vlastnosti** > **Přidat ...**.

ii) V okně Vybrat uživatele, počítače nebo skupiny zadejte *wmquser1; wmquser2* a klepněte na volbu **Zkontrolovat názvy**.

iii) V okně Zabezpečení systému Windows zadejte jméno a heslo administrátora domény a poté klepněte na tlačítko **OK** > **OK** > **Použít** > **OK**.

2. Otevřete příkazový řádek.
3. Restartujte službu IBM IBM WebSphere MQ .

   Službu musíte restartovat, aby ID uživatele, pod kterým je spuštěna, získalo další pověření zabezpečení, která jste pro ni nakonfigurovali.

   Zadejte příkazy:

   ```
   endmqsvc
   strmqsvc
   ```

   Odezvy systému:

   ```
   5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
   The MQ service for installation 'Installation1' ended successfully.
   A:
   5724-H72 (C) Copyright IBM Corp. 1994, 2024. 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, abyste povolili lokálnímu uživateli *user* přístup pro čtení a zápis.

   ```
   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 pro realistickou produkční konfiguraci pokračujte s ID uživatele s omezenějšími právy. ID uživatele musí být alespoň členem lokální skupiny mqm .

   Pokud je instalace produktu IBM WebSphere MQ konfigurována jako součást domény, učiňte ID uživatele členem skupiny Domain mqm . Průvodce "Připravit IBM WebSphere MQ" učiní globální skupinu Domain mqm členem lokální skupiny mqm , takže nemusíte přímo nastavit ID uživatele jako člena 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:

   ```
   WebSphere 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 se adresáře vytvořené správcem front nacházejí v adresáři *c:\wmq* .

   ```
   dir c:\wmq /D /B /S
   ```
9. Zkontrolujte, zda mají soubory oprávnění ke čtení a zápisu nebo úplné řízení pro lokální skupinu mqm .

```
cacls c:\wmq\*.*
```

Jak pokračovat dále

Otestujte správce front vložením a získáním zprávy do fronty.

1. Spusťte správce front.

   ```
   strmqm QMGR
   ```

   Odezva systému:

   ```
   WebSphere 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'.
   WebSphere 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, 2024. ALL RIGHTS RESERVED.
   Starting MQSC for queue manager QMGR.


        1 : define qlocal(QTEST)
   AMQ8006: WebSphere 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:

```
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

```
WebSphere MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

Tip: Přidejte volbu `/Q` k příkazům, abyste zabránili náznaku příkazu k odstranění každého souboru nebo adresáře.

```
del /F /S C:\wmq\*.*
rmdir /S C:\wmq
```

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. Kroky se liší na jiných platformách UNIX .

Příklad je nastaven na 2 GHz přenosný počítač se 3 GB RAM s operačním systémem Windows XP Service Pack 2. 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 je nainstalován na dalších 400 MB obrazu VMware , který spouští Windows XP s aktualizací Service Pack 2 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 NFSpoužijte k zajištění zabezpečení systému následující tři volby s příkazem mount:

neexec
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.

Příklad

Tabulka 30. Ilustrativní konfigurace správce front pro více instancí v systému Linux

Server1	Server2
Přihlaste se jako uživatel *root* .	
Postupujte podle pokynů v tématu Instalace produktu IBM WebSphere MQ k instalaci produktu WebSphere MQ, vytvořte uživatele mqm a skupinu, pokud tyto neexistují, a definujte `/var/mqm`. Podívejte se, co `uid` a `gid` v `/etc/passwd` na prvním počítači se zobrazí pro mqm; například, `mqm:x:501:100:MQ User:/var/mqm:/bin/bash` Porovnejte `uid` a `gid` pro mqm v `/etc/passwd` na druhém počítači, abyste se ujistili, že tyto hodnoty jsou identické. Restartujte tento počítač, pokud je třeba změnit hodnoty.	

Tabulka 30. Ilustrativní konfigurace správce front pro více instancí v systému Linux (pokračování)

Server1	Server2
Dokončete úlohu Ověření chování sdíleného systému souborů a zkontrolujte, zda systém souborů podporuje správce front s více instancemi.	
Vytvořte protokol a datové adresáře ve společné složce /MQHA, která má být sdílena. Příklad: 1. **mkdir** */MQHA* 2. **mkdir** */MQHA/logs* 3. **mkdir** */MQHA/qmgrs*	Vytvořte složku, /MQHA, chcete-li připojit sdílený systém souborů. Ponechte cestu stejně jako na serveru Server1; například: 1. **mkdir** */MQHA*
Ujistěte se, že adresáře MQHA jsou vlastněny uživatelem a skupinou mqm a přístupová oprávnění jsou pro uživatele a skupinu nastavena na rwx ; například se zobrazí **ls -al** , `drwxrwxr-x mqm mqm 4096 Nov 27 14:38 MQDATA` 1. **chown -R** mqm:mqm */MQHA* 2. **chmod -R** ug+rwx */MQHA*	
Vytvořte správce front: **crtmqm -ld** */MQHA/logs* **-md** */MQHA/qmgrs* *QM1*	
Přičíst[2] /MQHA *(rw,sync,no_wdelay,fsid=0) na /etc/exports	
Spusťte démona NFS : */etc/init.d/***nfs** start	Připojte exportovaný systém souborů /MQHA: **mount -t** nfs4 **-o** hard,intr *Server1:/ /MQHA*

Zkopírujte podrobnosti o konfiguraci správce front ze serveru Server1: .
`dspmqinf -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`
	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`

Spouštět instance správce front v jednom pořadí s parametrem **-x** : **strmqm** -x QM1 Příkaz používaný ke spuštění instancí správce front musí být zadán ze stejné instalace produktu IBM WebSphere 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.

[2] Volba '*' povoluje všechny počítače, které mohou dosáhnout tohoto připojení /MQHA pro čtení/zápis. Omezte přístup na produkční počítač.

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 373. 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 XP Service Pack 2. Systém hostuje dva servery VMware Linux , na kterých běží správce front s více instancemi.

Ověření překonání selhání pomocí Průzkumníka produktu WebSphere MQ

Než použijete ukázkové aplikace k ověření překonání selhání, spusťte na každém serveru produkt WebSphere MQ Explorer. 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 `mqm`je 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)
```

Případně můžete použít Průzkumníka WebSphere MQ Explorer, který je spuštěn modulem 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 amqsghac TARGET QM1
start amqsmhac -s SOURCE -t TARGET -m QM1
start amqsphac SOURCE QM1
```

Na serveru, na kterém je spuštěna aktivní instance správce front

1. Proveďte jednu z následujících akcí:
   - Zavřete okno se spuštěnou instancí serveru VMware s obrazem aktivního serveru.
   - Pomocí Průzkumníka produktu WebSphere MQ zastavte aktivní instanci správce front, což umožňuje přepnutí na záložní instanci a instruování opakovaného připojení klientů 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 všechna tři spojení znovu zavedne. 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:\>amqsghac 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 `mqs.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 `mqs.ini` . Je třeba navštívit každý server a odstranit sekci správce front spuštěním příkazu **rmvmqinf** *název oddílu správce front*.

Pokud jste v systémech UNIX and Linux umístili společný soubor `mqs.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 `mqs.ini` .

Příklad

První server

dltmqm QM1

Další servery, kde jsou definovány instance

rmvmqinf QM1nebo

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 *aktivním 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. Spustíte-li dvě instance zároveň, produkt WebSphere 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 spouštění.

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.
- Zálohujte lineární protokoly produktu WebSphere MQ na alternativní média, a pokud se vaše primární médium protokolu nezdaří, obnovte 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 přepnutí

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` . Třídy WebSphere MQ pro jazyk Java automatické opětovné připojování klientů nepodporují.

Pokud zjistíte, že nelze restartovat instanci, která selhala, i když došlo k překonání selhání a záložní instance se stala aktivní, zkontrolujte, zda se aplikace připojené lokálně k selhání instance neodpojily od nezdařené instance. Lokálně připojené aplikace jsou ukončeny nebo odpojeny od selhané instance správce front, aby bylo jisté, že instance se selháním může být restartována. 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 WebSphere 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. Třídy WebSphere MQ pro jazyk Java automatické opětovné připojování klientů nepodporují.

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. Znovu připojení produktu WebSphere MQ nelze změnit nebo přesměrovat 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 konfigurujte 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. Další informace o opětovném připojení klienta k správci front s více instancemi viz “Automatické opětovné připojení klienta” na stránce 301. Je třeba, aby klienti byli kompilovány ke spuštění s klientskými knihovnami produktu WebSphere MQ verze 7.0.1 nebo lépe. Musí být připojeny alespoň ke správci front 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 obnovování aplikace ztrácí kontext, který je sdílen mezi klientem WebSphere MQ MQI a správcem front a je uložen ve správci front. Klient WebSphere MQ MQI obnovuje většinu kontextu, ale některé části kontextu, které nelze spolehlivě obnovit, jsou některé části. 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 WebSphere 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 reconnectable aplikace kód příčiny MQRC_BACKED_OUT , aby indikoval, že transakce se nezdařila, a potřebuje odvolat transakci vydáním příkazu MQBACK. 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*. Třídy WebSphere MQ pro jazyk Java automatické opětovné připojování klientů nepodporují.

S aplikací klienta WebSphere MQ MQI 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 WebSphere MQ se při selhání instance správce front s více instancemi zpravidla nerestartuje na instanci správce front v pohotovostním režimu.

Server WebSphere MQ můžete automatizovat tak, 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 klienta WebSphere MQ MQI 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 vydáním MQBACK a restartováním jednotky práce, pak se neztratí žádné zprávy. 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 části “Zotavení automaticky znovu připojeného klienta” na stránce 382.

Pro klientské aplikace WebSphere MQ MQI jsou k dispozici tři alternativní vzory návrhu 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 zahodit všechny informace o stavu produktu WebSphere MQ , jako jsou například obslužné rutiny fronty, a vydat nové volání produktu MQCONN nebo MQCONNX k vytvoření nového připojení a poté znovu otevřít objekty produktu WebSphere 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.

Reconnuction aware

Zaregistrujte obslužnou rutinu událostí MQCBT_EVENT_HANLER 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 381pro klienta WebSphere MQ MQI 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. Je třeba vědět, jak opětovné připojení změní stav klienta WebSphere MQ MQI s cílem 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 rozpoznání tohoto opětovného připojení a registraci obslužné rutiny událostí s produktem WebSphere 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 klienta WebSphere MQ MQI si je vědomy samotného překonání selhání a obnovuje se tak, jak může, po opětovném připojení, uložením některých informací o stavu v klientovi a vydáním dalších volání MQI pro účely obnovení stavu WebSphere MQ v zastoupení aplikace klienta. Například jsou obnoveny

objekty, které byly otevřené v bodu selhání, a dočasné dynamické fronty se otevírají 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 navrženým způsobem a relegují méně časté chyby na generickou obslužnou rutinu chyb. Obslužná rutina chyb se může odpojit od produktu WebSphere MQ a znovu se připojit, nebo dokonce zastavit program úplně. Pro zlepšení kontinuity může být třeba řešit některé chyby v odlišném směru.
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 v případě, že klient WebSphere MQ MQI 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 klient WebSphere MQ MQI nepřijal 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, klient WebSphere MQ MQI nemůže znovu vytvořit dočasnou dynamickou frontu, protože ji nemá k vytvoření modelu. 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 MQPUT1nebo 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 se různé adresáře produktu WebSphere MQ mapují na paměťové médium, aby bylo co nejlépe využívat média. Pro správce front *více instancí* existuje důležité rozlišení mezi dvěma typy adresářů a souborů produktu WebSphere 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 *mají* 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 produktu WebSphere 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 WebSphere MQ, například souborem `mqs.ini` v systémech Windows, systémy UNIX and Linux nebo součástí vaší vlastní správy konfigurace, jako jsou 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 UNIX and Linux je `/var/mqm` . V systému Windows je výchozím datovým adresářem instalační adresář produktu `WebSphere 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 mechanizmus 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 WebSphere MQ
Aplikace používají jiné funkce produktu IBM WebSphere MQ ke zlepšení dostupnosti. Správci front s více instancemi doplňují jiné možnosti vysoké dostupnosti.

IBM WebSphere 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 směrovány do jiných správců front v klastru, jsou směrovány 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 nepřerušenou službu. Nové zprávy přijaté klastrem se odešlou do aktivních správců front, které mají být zpracovány. Nespoléhejte 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 mechanizmů 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 systému 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 systému z/OS podporovány a doplňují skupiny sdílení front pouze jako součást širší architektury systému zpráv.

WebSphere MQ Klienti zvyšují dostupnost aplikací.

WebSphere MQ Klientské programy MQI se mohou připojit 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 vyrovnávání 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. Třídy WebSphere MQ pro jazyk Java automatické opětovné připojování klientů nepodporují.

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 opětovného 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)

Produkt WebSphere MQ protokoluje všechny informace, které potřebujete k zotavení ze selhání správce front.

Produkt WebSphere MQ zaznamenává všechny významné změny dat řízených správcem front v protokolu 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 WebSphere MQ se však také spoléhá na diskový systém, který je hostitelem jeho souborů. 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 produktu WebSphere 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 řada souborů protokolu, které obsahují zaznamenaná data. Můžete definovat počet a velikost (jak je vysvětleno v části “Změna konfiguračních informací IBM WebSphere MQ a správce front” na stránce 406), nebo můžete použít výchozí systémové soubory.

V produktu WebSphere MQ for Windowsje každý z těchto tří souborů standardně nastaven na 1 MB.
V systému WebSphere MQ pro systémy UNIX and Linux je každý z těchto tří souborů standardně nastaven na 4 MB.

Při vytváření správce front je k dispozici počet souborů protokolu, které definujete jako počet přidělených souborů protokolu *primární* . Pokud číslo nezadáte, použije se výchozí hodnota.

Pokud jste v produktu WebSphere MQ for Windowsnezměnili cestu k protokolu, soubory protokolu se vytvoří pod adresářem:

```
C:\Program Files\IBM\WebSphere MQ\log\<QMgrName>
```

Pokud jste v systému WebSphere MQ for UNIX and Linux nezměnili cestu k protokolu, soubory protokolu se vytvoří v adresáři:

```
/var/mqm/log/<QMgrName>
```

WebSphere MQ začíná těmito primárními soubory protokolů, ale pokud není primární prostor žurnálu dostatečný, alokuje *sekundární* soubory protokolu. To dělá dynamicky a odstraňuje je, když se sníží poptávka po protokolovaných prostorech. Standardně může být alokováno až dva sekundární soubory protokolu. Toto výchozí přidělení můžete změnit, jak je popsáno v tématu “Změna konfiguračních informací IBM WebSphere MQ a správce front” na stránce 406.

Soubor řízení žurnálu

Řídicí soubor protokolu obsahuje informace potřebné k řízení použití souborů protokolu, jako je jejich velikost a umístění, a název dalšího dostupného souboru.

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.

Poznámka: Ujistěte se, že protokoly vytvořené při spuštění správce front jsou dostatečně velké, aby vyhověly velikosti a objemu zpráv, které vaše aplikace zpracují. Pravděpodobně budete muset změnit výchozí počty protokolů a velikosti tak, aby splňovaly vaše požadavky. Další informace viz “Výpočet velikosti protokolu” na stránce 391.

Typy protokolování

V produktu WebSphere MQzávisí počet souborů, které jsou vyžadovány pro protokolování, na velikosti souboru, počtu přijatých zpráv a délce zpráv. 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 WebSphere 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 “Použití kontrolního bodu k zajištění úplné obnovy” na stránce 389.

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 udržuje data protokolu v kontinuální posloupnosti souborů. Nedochází k opětovnému využívání místa, takže lze protokolovaný záznam vždy načíst, pokud nebyl smazán.

Vzhledem k tomu, že prostor na disku je konečný, možná budete muset přemýšlet o nějaké formě archivace. Jedná se o administrativní úlohu pro správu místa na disku pro protokol, opětovné použití nebo rozšíření existujícího prostoru podle potřeby.

Počet souborů protokolu použitých s lineárním protokolováním může být velmi velký, v závislosti na toku zpráv a stáří vašeho správce front. Existuje však řada souborů, které se říká, že jsou *aktivní*. Aktivní soubory obsahují položky protokolu vyžadované k restartování správce front. Aktivní, aktivní soubory protokolu jsou známé jako *aktivní protokol*. 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 391 .)

Klíčová událost, která řídí, zda je soubor protokolu označen jako aktivní, či nikoli, je *kontrolní bod*. Kontrolní bod WebSphere MQ je bod konzistence mezi protokolem o zotavení a soubory objektů. Kontrolní bod určuje sadu souborů protokolů potřebných k provedení zotavení při restartu. Soubory protokolu, které nejsou aktivní, nejsou pro obnovu restartování nezbytné a jsou označovány jako neaktivní. V některých případech jsou neaktivní soubory protokolu vyžadovány pro obnovu médií. (Další informace o kontrolních bodech naleznete v tématu “Použití kontrolního bodu k zajištění úplné obnovy” na stránce 389 .)

Neaktivní soubory protokolu lze archivovat, protože nejsou pro zotavení restartovány. 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. Další informace o odebírání souborů protokolu najdete v tématu “Správa protokolů” na stránce 393 .

Je-li nový kontrolní bod zaznamenán ve druhém nebo pozdějším primárním souboru protokolu, první soubor se může stát neaktivním a nový primární soubor bude formátován a přidán do konce primárního fondu a obnoví se počet primárních souborů, které jsou k dispozici pro protokolování. Tímto způsobem může být primární fond souborů protokolu považován za aktuální sadu souborů v čím dál rozšiřujícím seznamu souborů protokolu. Opět je administrativní úloha pro správu neaktivních souborů v souladu s požadavky vaší operace.

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.

Je-li použit počet sekundárních souborů, které jsou k dispozici, jsou požadavky na většinu dalších operací vyžadujících aktivitu protokolu odmítnuty s návratovým kódem MQRC_RESOURCE_PROBLEM, který se vrací do aplikace.

Oba typy protokolování se mohou vypořádat s neočekávanou ztrátou výkonu za předpokladu, že nedošlo k žádnému selhání hardwaru.

Použití kontrolního bodu k zajištění úplné obnovy

Kontrolní body synchronizují data správce front a soubory protokolu a označují bod konzistence, ze kterého mohou být záznamy protokolu vyřazeny. Časté kontroly vedou k rychlejšímu zotavení.

Trvalé aktualizace front zpráv probíhá ve dvou fázích. Za prvé jsou záznamy představující aktualizaci zapsány do protokolu, pak je soubor fronty aktualizován. Soubory protokolu se tak mohou stát aktuálnější než soubory fronty. Chcete-li zajistit, aby zpracování restartování bylo zahájeno z konzistentního bodu, produkt WebSphere MQ používá kontrolní body. Kontrolní bod je bod v čase, kdy je záznam popsaný v protokolu stejný jako záznam ve frontě. Samotný kontrolní bod se skládá z řady záznamů protokolů potřebných k restartování správce front; například stav všech transakcí (jednotky práce) aktivních v době kontrolního bodu.

Produkt WebSphere MQ generuje kontrolní body automaticky.Jsou převzaty, když se správce front spustí, při vypnutí, kdy je protokolovací prostor nízký, a po každých 10 000 zaprotokolovaných operacích.

Protože fronty zpracovávají další zprávy, záznam kontrolního bodu se stane nekonzistentní s aktuálním stavem front.

Po restartování produktu WebSphere MQ vyhledá poslední záznam kontrolního bodu v protokolu. Tyto informace jsou uloženy v souboru kontrolního bodu, který je aktualizován na konci každého kontrolního bodu. Záznam kontrolního bodu představuje nejnovější bod konzistence mezi protokolem a daty. 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. Vydávají se zprávy AMQ7229 a AMQ7230 , které označují průběh fáze přehrávání.

Chcete-li zjistit, které operace mají být vraceny nebo potvrzeny, produkt WebSphere MQ přistupuje ke každému aktivnímu záznamu protokolu přidruženému k transakci v rámci letu. Tento stav je znám jako fáze obnovení. Zprávy AMQ7231, AMQ7232 a AMQ7234 jsou vydávány s cílem označit průběh fáze obnovení.

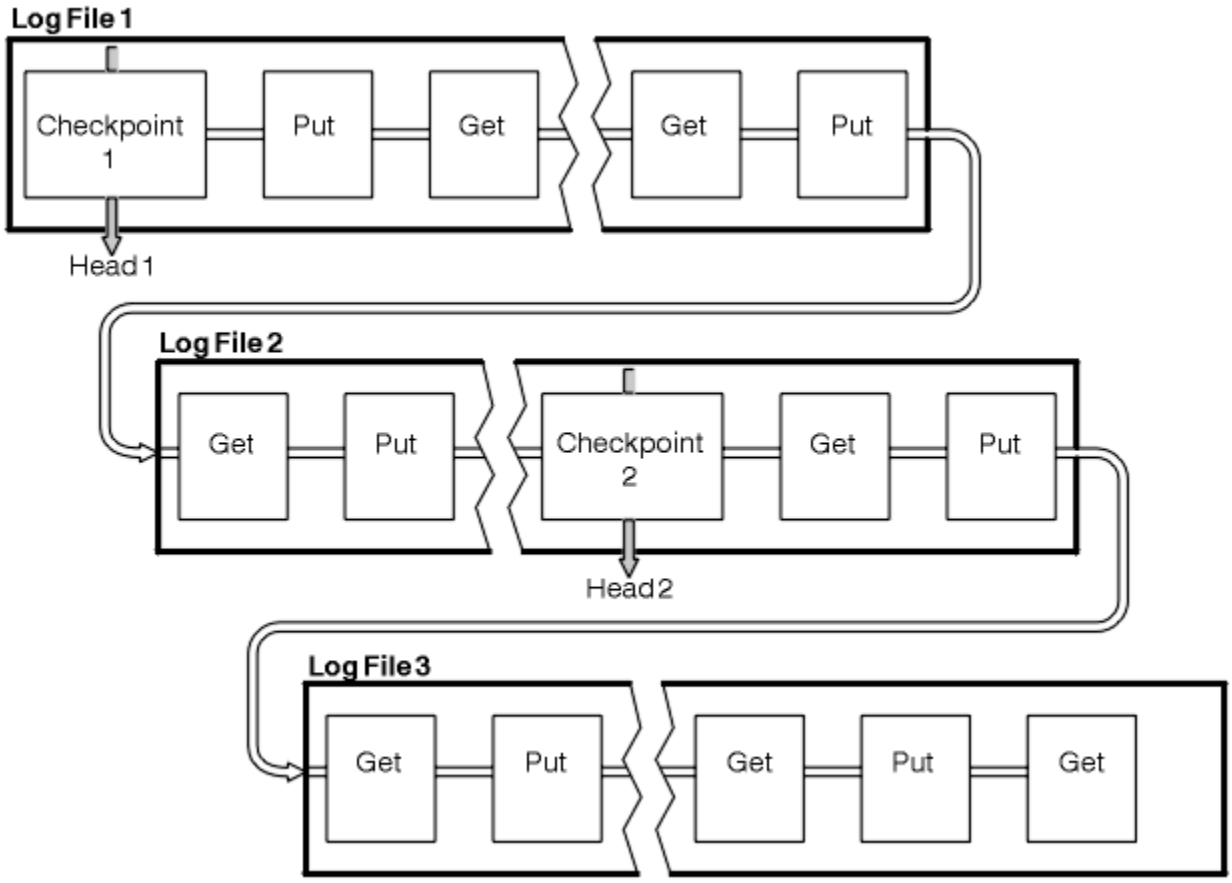
Jakmile jsou k dispozici všechny potřebné záznamy protokolu během fáze obnovy, každá aktivní transakce se zase vyřeší a každá operace přidružená k transakci bude buď vrácena, nebo potvrzena. To je známo jako fáze řešení. Byla vydána zpráva AMQ7233 , která označuje průběh fáze rozpoznání.

Produkt WebSphere MQ udržuje interní ukazatele na záhlaví a zápatí protokolu. Pohybuje ukazatel hlavy na nejnovější kontrolní bod konzistentní s obnovujícími daty zprávy.

Kontrolní body se používají k účinnějšímu využití zotavení a k řízení opětovného použití primárních a sekundárních souborů protokolu.

V produktu Obrázek 69 na stránce 390nejsou všechny záznamy před posledním kontrolním bodem 2, kontrolního bodu 2, již nadále vyžadovány produktem WebSphere MQ. 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 69. Ukládám

Kontrola s dlouhotrvanými transakcemi

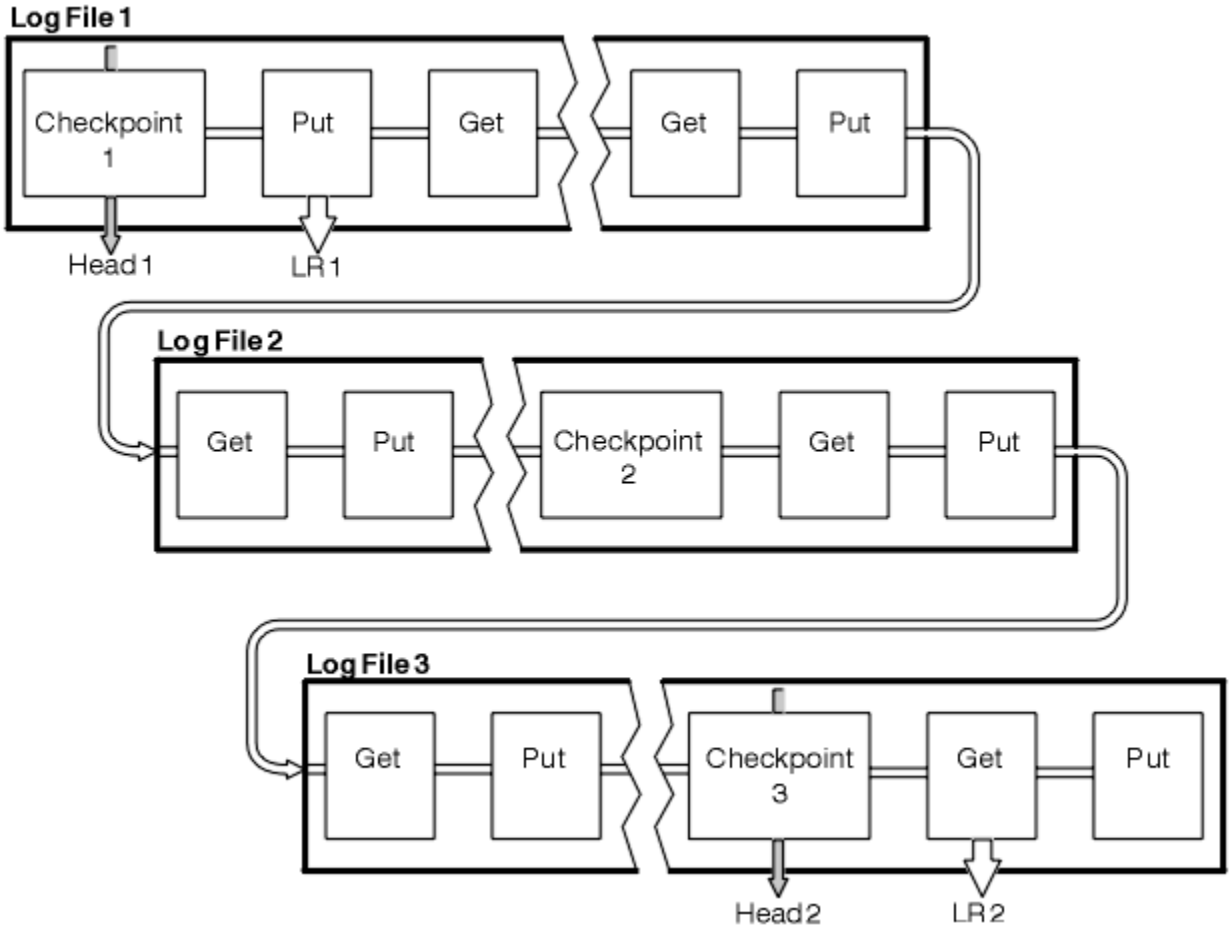
Jak dlouho běžící transakce ovlivňuje opětovné použití souborů protokolu.

Příkaz Obrázek 70 na stránce 391 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 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 soubory primárního protokolu zcela zaplněna před dokončením transakce s dlouhou dobou zpracování, sekundární soubory protokolu se používají, aby nedošlo k zaplnění protokolů.

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 70. 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 protokolu, který správce front potřebuje. Velikost protokolu je určena následujícími parametry konfigurace 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, když jsou primární soubory protokolu plné

Tabulka 31 na stránce 392 uvádí množství dat, které správce front protokoluje pro různé operace. Většina operací správce front potřebuje minimální množství protokolovacího prostoru.Je-li však do fronty vložena trvalá zpráva, musí být data zprávy zapsána do protokolu **všechna** , aby bylo možné zprávu obnovit. Velikost protokolu závisí obvykle na počtu a velikosti trvalých zpráv, které správce front potřebuje zpracovat.

Tabulka 31. Velikosti záznamu žurnálu (všechny hodnoty jsou přibližné)	
Operace	**Velikost**
Vložit trvalou zprávu	750 bajtů + délka zprávy Je-li zpráva velká, je rozdělena do segmentů 261844 bajtů, každý segment přidává dalších 300 bajtů.
Získat zprávu	260 bajtů
Bod synchronizace, potvrzení	750 bajtů
Bod synchronizace, odvolání	1000 bajtů + 12 bajtů pro každé získání nebo vložení, které mají být odvolány
Vytvořit objekt	1500 bajtů
Odstranit objekt	300 bajtů
Změnit atributy	1024 bajtů
Zaznamenat obraz média	800 bajtů + obraz Obraz je rozdělen do segmentů o velikosti 260 000 bajtů, každý segment přidává dalších 300 bajtů.
Kontrolní bod	750 bajtů + 200 bajtů pro každou aktivní jednotku práce + 380 bajtů pro každý odesílací kanál klastru, pokud používáte více přenosových front klastru pro každého správce front. Další data mohou být protokolována pro nepotvrzené operace vložení nebo získání, které jsou z důvodu výkonu uloženy do vyrovnávací paměti. Pokud máte odesílací kanály klastru, pak se na každém kontrolním bodu zapíše do protokolu počet dalších 380 bajtů na kanál odesílacího kanálu klastru.

Poznámka:

1. Můžete změnit počet primárních a sekundárních souborů protokolu pokaždé, když se správce front spustí.
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 UNIX and Linux nebo 255 v systému 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 prostor žurnálu. To znamená, že protokol správce front může být menší než objem dat, která jste odhadovali, že správce front se musí protokolovat. 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.
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.

   Pokud nedefinujete více souborů primárního protokolu než sekundární soubory žurnálu, může správce front před přijetím kontrolního bodu přidělit sekundární soubory protokolu. Tím jsou primární soubory žurnálu k dispozici pro opětovné použití.

Správa protokolů

Protokoly jsou téměř samoobslužné, ale někdy potřebují spravovat, aby se vyřešily problémy s prostorem.

V průběhu času se některé zapsané záznamy protokolu stanou pro restartování správce front nepotřebnými. Pokud používáte kruhové protokolování, správce front uvolní prostor v souborech protokolu. Tato aktivita není uživateli zřejmá a obvykle se nezobrazuje množství využitého místa na disku, protože přidělený prostor je rychle znovu využit.

Ze záznamů protokolu jsou k restartování správce front potřeba pouze ty, které byly zapsány od začátku posledního dokončeného kontrolního bodu, a ty, které byly zapsány aktivními transakcemi. Protokol se tedy může zaplnit, pokud nebyl kontrolní bod již dlouho vzat, nebo pokud dlouho trvající transakce zapsala záznam protokolu. Správce front se pokusí převzít kontrolní body dostatečně často, aby se vyhnul prvnímu problému.

Při zaplnění protokolu přerušitelnou transakcí dojde k selhání pokusů o zápis záznamů protokolu a některá volání MQI vrátí chybu MQRC_RESOURCE_PROBLEM. (Prostor je vyhrazen pro potvrzení nebo odvolání všech probíhajících transakcí, takže **MQCMIT** nebo **MQBACK** by nemělo selhat.)

Správce front odvolá transakce, které spotřebovávají příliš mnoho protokolovacího prostoru. Aplikace, která má transakci, je tímto způsobem odvolána, nemůže provádět následné operace **MQPUT** nebo **MQGET** určující synchronizační bod v rámci stejné transakce. Pokus o vložení nebo získání zprávy do synchronizačního bodu v tomto stavu vrací 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 protokolovacího prostoru, dojde k uvolnění příslušného protokolovacího prostoru a správce front bude i nadále pracovat normálně.

Pokud se protokol zaplní, vydá se zpráva AMQ7463 . Kromě toho, pokud se protokol zaplní, protože přerušitelná transakce zabránila uvolnění prostoru, vydá se zpráva AMQ7465 .

Nakonec, pokud jsou záznamy zapisovány do protokolu rychleji, než je může protokol zpracovat, je vydána zpráva AMQ7466 . Zobrazí-li se tato zpráva, zvyšte počet souborů protokolu nebo snižte množství dat zpracovávaných správcem front.

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, který obsahuje protokol, zaplní, vydá správce front zprávu AMQ6708 a bude proveden záznam o chybě.

Soubory protokolu se vytvářejí při jejich maximální velikosti, místo aby byly rozšířeny, aby se do nich zapsali záznamy protokolu. To znamená, že produkt WebSphere MQ může mít nedostatek místa na disku pouze v případě, že vytváří nový soubor. Při zápisu záznamu do protokolu nemůže dojít k nedostatku prostoru. Produkt WebSphere 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. 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 předpokládá, že všechny soubory protokolu mají stejnou velikost.

Správa souborů protokolu

Alokujte dostatečný prostor pro vaše soubory protokolů. Pro lineární protokolování můžete odstranit staré soubory protokolu, když již nejsou potřeba.

Používáte-li kruhové protokolování, ujistěte se, že je dostatek místa pro uchování souborů protokolu při konfiguraci systému (viz “Předvolby protokolu pro IBM WebSphere MQ” na stránce 414 a “Protokoly správce front” na stránce 422). Množství prostoru na disku použitého protokolem se nezvýší za nakonfigurovanou velikost, včetně prostoru pro sekundární soubory, které mají být vytvořeny, když je to požadováno.

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 jakýmikoli poškozenými objekty. Pro určení, které soubory protokolu jsou stále vyžadovány, jsou tyto metody:

Zprávy událostí modulu protokolování
Je-li tato volba povolena, jsou zprávy událostí modulu protokolování generovány, když správce front zahájí zápis záznamů protokolu do nového souboru protokolu. 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 AMQ7467 uvádí 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 AMQ7468 uvádí název nejstaršího souboru protokolu potřebného pro zotavení média.

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.

Chcete-li určit "starší" a "novější" soubory protokolu, použijte místo úpravy, které používá systém souborů, číslo souboru protokolu.

Pokud nelze najít žádný potřebný soubor protokolu, vydá se zpráva operátora AMQ6767 . Vytvořte soubor protokolu a všechny následné soubory protokolu dostupné pro správce front a zkuste operaci zopakovat.

Poznámka: Při provádění obnovení 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 vytvořit obraz média všech objektů ve správci front, spusťte příkaz **rcdmqimg** , jak ukazuje následující příklady:

V systémech Windows

```
rcdmqimg -m QMNAME -t all *
```

V systému UNIX and Linux

```
rcdmqimg -m QMNAME -t all "*"
```

Spuštění **rcdmqimg** 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 398. **rcdmqimg** se nespustí automaticky, proto musí být spuštěn ručně nebo z automatické úlohy, kterou jste vytvořili. Další informace o tomto příkazu naleznete v části rcdmqimg a dmpmqlog.

Poznámka: Zprávy AMQ7467 a AMQ7468 mohou být také vydávány v době spuštění příkazu `rcdmqimg` .

Určení nadbytečných souborů protokolu
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 časy úpravy, které by byly zavádějící.

Chcete-li určit nejstarší soubor protokolu potřebný k restartování správce front, zadejte příkaz `DISPLAY QMSTATUS RECLOG`.

Chcete-li určit nejstarší soubor protokolu potřebný k provedení zotavení média, 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, pak nemusíte obstarávat počet balení 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.

Pokud však máte velmi vysoký obrat souborů protokolu, nebo se chcete spolehnout na to, že se s obecným případem vypořádá, lze obvykle použít následující algoritmus:

```
Let S == restartovat číslo souboru protokolu
         (z DISPLAY QMSTATUS RECLOG).
Let M == číslo souboru protokolu pro zotavení médií
          (z DISPLAY QMSTATUS MEDIALOG).
Nechť L == a číslo souboru protokolu se způsobilostí pro odstranění nebo archivaci
           který je třeba určit.

funkce minlog (a, b) {
  if (abs (a-b) < 5000000)
    return min (a, b); # Not wrapped.
  else
    return max (a, b); # Wrapped.}

Soubor protokolu L lze odstranit, pokud
       (L! = S & & L! = M & & minlog (L, minlog (S, M)) == L).
Soubor protokolu L může být archivován, pokud
       (L! = S & & minlog (L, S) == L).
```

Umístění souboru žurnálu

Při výběru umístění pro soubory protokolu pamatujte na to, že operace je výrazně ovlivněna, pokud produkt WebSphere 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.

V ideálním případě umístěte soubory protokolu na samostatnou diskovou jednotku z dat správce front. To má přínos z hlediska výkonu. Může být také možné umístit soubory protokolu na více diskových jednotek v zrcadleném uspořádání. To chrání před selháním jednotky, která obsahuje protokol. Bez zrcadlení můžete být nuceni vrátit se zpět k poslední záloze vašeho systému WebSphere MQ .

Použití protokolu pro zotavení

Použití protokolů k zotavení ze selhání.

Existuje několik způsobů, jak mohou být vaše data poškozena. Produkt WebSphere MQ vám pomůže provést zotavení:

- 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

WebSphere MQ se může zotavit z obou selhání komunikací a ztráty moci. Kromě toho se může někdy zotavit z jiných typů problémů, jako je například neúmyslné odstranění souboru.

V případě selhání komunikace zprávy zůstávají ve frontě, 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.

Pokud při restartování správce front dojde ke ztrátě napájení, produkt WebSphere MQ obnoví fronty do jejich potvrzeného stavu v době selhání. Tím je zajištěno, že žádné trvalé zprávy nebudou ztraceny. Netrvalé zprávy jsou zahozeny. Nepřetrvají při náhlém zastavení produktu WebSphere MQ .

Obnova poškozených objektů

Existují způsoby, jak může být objekt IBM WebSphere 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 média

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 média 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 WebSphere 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 WebSphere 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 WebSphere MQ poškozen, jediné platné akce, které lze provést, je buď odstranit, nebo znovu vytvořit touto metodou. 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 WebSphere 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 WebSphere 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 WebSphere 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 WebSphere MQ . Pokud uživatel neúmyslně odstraní soubory protokolu, které správce front potřebuje restartovat, produkt IBM WebSphere 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 WebSphere MQ). Mohou tedy poškodit běžící nebo nečinné správce front způsobem, který nedokáže ochránit sám IBM WebSphere MQ .

Dávejte pozor při udělování superuživatele nebo oprávnění mqm.

Výpis obsahu protokolu pomocí příkazu dmpmqlog

Chcete-li vypsat obsah protokolu správce front, použijte příkaz dmpmqlog k výpisu obsahu protokolu správce front.

Chcete-li vypsat 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 vypsat 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 vypsaných 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 úrovní 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 bází 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:

logactive	Počet oblastí primárního protokolu.
loginactive	Počet sekundárních fyzických oblastí protokolu.
velikost_protokolu	Počet stránek o velikosti 4 kB za fyzickou oblast.
základ_sn	První LSN v rozsahu protokolu obsahující hlavu protokolu.
nextlsn	Pořadové číslo LSN dalšího záznamu protokolu, který má být zapsán.
headlsn	Pořadové číslo protokolu záznamu v protokolu v záhlaví protokolu.

tailsn Pořadové číslo v protokolu LSN označující koncovou pozici protokolu v protokolu.

hflag1 Zda se jedná o protokol CIRCULAR nebo LOG RETAIN (lineární).

IDHeadExtentID Oblast protokolu obsahující hlavičku protokolu.

Záhlaví záznamu protokolu

Každý záznam protokolu v rámci protokolu má pevné záhlaví obsahující následující informace:

LSN Pořadové číslo v protokolu.

LogRecdTyp Typ záznamu protokolu.

XTrand Identifikátor transakce přidružený k tomuto záznamu protokolu (pokud existuje).

TranType rozhraní MQI označuje transakci WebSphere MQ-only. *TranType* z XA se podílí na jiných správcích prostředků. Aktualizace zahrnuté do stejné jednotky práce mají stejný *XTranid*.

QueueName Fronta přidružená k tomuto záznamu protokolu (pokud existuje).

Qid Jedinečný vnitřní identifikátor fronty.

PrevLSN Pořadové číslo předchozího záznamu protokolu v protokolu v rámci stejné transakce (je-li k tomu došlo).

Spustit správce front

Protokoly, které správce front spustil.

StartDate Datum, kdy byl spuštěn správce front.

StartTime Čas, kdy byl správce front spuštěn.

Zastavit správce front

Protokoly, které správce front zastavily.

StopDate Datum, kdy byl zastaven správce front.

StopTime Čas zastavení správce front.

ForceFlag Typ použitého ukončení práce.

Začátek kontrolního bodu

To označuje začátek kontrolního bodu správce front.

Koncový kontrolní bod

To označuje konec kontrolního bodu správce front.

ChkPtLSN 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:

MapIndex 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 *Get Message* obsahující stejné QueueName a MapIndex. V tomto okamžiku lze identifikátor MapIndex znovu použít pro následné vložení zprávy do této fronty.

Data Obsaženo v hexadecimálním výpisu paměti pro tento záznam protokolu je různá vnitřní data, za nimiž následují deskriptor zprávy (eyecatcher MD) a 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 zřetězit záznamy *Put Part* a konečný záznam *Put Message* dohromady.

Data 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:

MapIndex Identifikuje zprávu, která byla načtena z fronty. Nejnovější záznam protokolu *Put Message* obsahující stejné *QueueName* a *MapIndex* identifikuje zprávu, která byla načtena.

QPriority Priorita zprávy načtené z fronty.

Spustit transakci

Označuje začátek nové transakce. TranType rozhraní MQI označuje transakci pouze pro WebSphere 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:

XTrand Identifikátor transakce.

FirstLSN Pořadové číslo v protokolu prvního záznamu protokolu přidruženého k transakci.

LastLSN 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:

RMName Název správce prostředků.

RMID	Identifikátor správce prostředků. To je také zaprotokolováno v následných záznamech protokolu *Transaction Prepared* , které zaznamenávají globální transakce, v nichž se správce prostředků podílí.
SwitchFile	Soubor načtení přepínače pro tohoto správce prostředků.
XAOpenString	Otevřený řetězec XA pro tohoto správce prostředků.
XACloseString	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 WebSphere MQ .

ObjName	Název objektu, který byl vytvořen.
UserId	ID uživatele, který provádí vytvoření.

Odstranit objekt
Tím se protokolují odstranění objektu WebSphere MQ .

ObjName	Název objektu, který byl odstraněn.

Zálohování a obnova dat správce front produktu IBM WebSphere 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 402.
- “Obnova dat správce front” na stránce 403.

Použít 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 404.
- "Spuštění záložního správce front" na stránce 405.

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 405
- "Obnovení konfigurace správce front" na stránce 406

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 umisťuje svá data a soubory protokolu za použití informací v konfiguračních souborech. Další informace viz "Změna konfiguračních informací IBM WebSphere MQ a správce front" na stránce 406.

   Poznámka: Možná budete mít určité potíže s pochopeni se jmény, která se objevují v adresáři. Názvy se transformují, aby se ujistili, že jsou kompatibilní s platformou, na které používáte produkt WebSphere MQ. Další informace o transformacích názvů najdete v tématu Základní informace o názvech souborů produktu WebSphere MQ.
2. Převeďte 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 387, a konfigurační soubory, jak je popsáno v tématu "Inicializační a konfigurační soubory" na stránce 68. Některé adresáře mohou být prázdné, ale vy je budete potřebovat k obnovení zálohy později.
3. Zachovejte vlastnictví souborů. Pro systémy WebSphere MQ for UNIX and Linux lze tuto akci provést pomocí příkazu `tar` . (Máte-li fronty větší než 2 GB, nelze použít příkaz `tar` . Další informace naleznete v tématu Povolení velkých front.

Poznámka: Když upgradujete na produkt WebSphere MQ verze 7.5 a novější, 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 opětovnému vrácení na předchozí verzi produktu WebSphere 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.

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 umisťuje 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 WebSphere MQ viz Adresářová struktura v systémech Windows a Obsah adresáře v systémech UNIX and Linux .

Ujistěte se, že máte soubor s řízením protokolu a také soubory protokolu. Dále zkontrolujte, zda jsou konfigurační soubory produktu IBM WebSphere MQ a správce front konzistentní, takže produkt WebSphere 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: Když upgradujete na produkt WebSphere MQ verze 7.5 a novější, 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 opětovnému vrácení na předchozí verzi produktu WebSphere 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. Jakmile je správce front zálohování aktivován, nelze jej již aktualizovat.

Informace o tom, jak vytvořit, aktualizovat a spustit správce front zálohování, najdete v následujících tématech:

- “Vytvoření správce front zálohování” na stránce 404
- “Aktualizace záložního správce front” na stránce 404
- “Spuštění záložního správce front” na stránce 405

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 `crtmqm`. 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 402.
3. Přepište soubory dat a adresáře souborů správce front zálohování, včetně všech podadresářů, s kopiemi převzatovanými z existujícího správce front.
4. Proveďte následující řídicí příkaz na správci front zálohování:

   ```
   strmqm -r BackupQMName
   ```

   Tento příznak označí správce front jako správce front zálohy v rámci produktu WebSphere MQa přehraje všechny zkopírované oblasti protokolu, aby správce front v kroku s existujícím správcem front mohl být správcem front zkopírován.

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:

```
strmqm -r 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:

```
strmqm -a BackupQMName
```

   Záložní správce front je aktivován. Aktivní správce front zálohy již nelze aktualizovat.
2. Spuštěním následujícího příkazu ovládacího prvku spusťte správce front zálohování:

```
strmqm BackupQMName
```

   Produkt WebSphere MQ považuje toto zotavení za restartování a využívá protokol ze správce front zálohování. Během poslední aktualizace pro přehrání 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 WebSphere MQ naleznete v tématu Plánování podpory systému souborů .

Ujistěte se, že máte soubor s řízením protokolu a také soubory protokolu. Dále zkontrolujte, zda jsou konfigurační soubory produktu WebSphere MQ a správce front konzistentní, takže produkt WebSphere MQ může vyhledávat obnovená data na správných místech.

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. V systému AIX, HP-UX, Linux, Solaris nebo Windows: Spusťte příkaz MQ Configuration (dmpmqcfg) pomocí výchozí volby formátování (-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
```

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 systému AIX, HP-UX, Linux, Solaris nebo Windows: Execute runmqsc against the queue manager, use standard input redirection to restore the definitions from a script file generated by the Dump MQ Configuration (dmpmqcfg) command, for example:

```
runmqsc MYQMGR < /mq/backups/MYQMGR.mqsc
```

Související odkazy

dmpmqcfg

Změna konfiguračních informací IBM WebSphere MQ a správce front

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

Informace o konfiguraci produktu IBM WebSphere MQ můžete změnit tak, že změníte hodnoty zadané na sadě konfiguračních atributů (nebo parametrů), které řídí IBM WebSphere MQ.

Změňte informace o atributu upravením konfiguračních souborů produktu IBM WebSphere MQ . Na systémech IBM WebSphere MQ pro produkty Windows a Linux (platformyx86 a x86-64) lze konfigurační soubory produktu IBM WebSphere MQ upravovat pomocí produktu IBM WebSphere MQ Explorer.

Na systémech Windows můžete také použít amqmdain pro změnu konfiguračních informací, jak je popsáno v amqmdain

Další informace o konfiguraci produktu IBM WebSphere 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.

Související úlohy

Naplánování

Správa produktu WebSphere MQ

Změna konfiguračních informací v systémech UNIX, Linux, and Windows

Konfigurační atributy se nacházejí v konfiguračních souborech, na úrovni uzlu a správce front.

Na platformách Windows, UNIX and Linux můžete změnit atributy konfigurace produktu IBM WebSphere MQ v rámci následujících položek:

- Konfigurační soubor produktu IBM WebSphere MQ (**mqs.ini**), který ovlivní změny pro IBM WebSphere MQ na uzlu jako celku. Pro každý uzel je k dispozici jeden soubor mqs.ini .
- Konfigurační soubor správce front (**qm.ini**) pro provedení změn pro specifické správce front. Pro každého správce front v daném uzlu existuje jeden soubor qm.ini .

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 WebSphere 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 WebSphere MQ .

Jakékoli změny, které provedete v konfiguračním souboru, se obvykle projeví až po příštím spuštění správce front.

V systémech Windows a Linux (platformyx86 a x86-64) můžete upravit informace o konfiguraci z pohledu IBM WebSphere MQ Explorer.

Na systémech Windows můžete také použít příkaz `amqmdain` k úpravě konfiguračních souborů.

Další informace o volbách konfigurace v systémech Windows, UNIX and 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 WebSphere MQ a správce front” na stránce 406
Změňte chování produktu IBM WebSphere MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související úlohy

Naplánování

Správa produktu WebSphere MQ

Související odkazy

“Atributy pro změnu konfiguračních informací IBM WebSphere MQ” na stránce 412
V systému IBM WebSphere MQ pro systémy Windows a v systémech IBM WebSphere MQ for Linux (platformyx86 a x86-64) upravte informace o konfiguraci pomocí produktu IBM WebSphere MQ Explorer. V jiných systémech upravte informace úpravou konfiguračního souboru mqs.ini .

“Změna konfiguračních informací správce front” na stránce 418
Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro produkt WebSphere 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 WebSphere 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:

- Vytvořte zálohu konfiguračního souboru produktu WebSphere 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?

Editujte konfigurační soubor pro obnovu ze zálohy, přesuňte správce front, změňte výchozího správce front nebo napomůže podpoře 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.
- Doporučujeme vám to servisní středisko IBM Support Center.

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 WebSphere MQ , mqs.ini .

Konfigurační soubor IBM WebSphere MQ mqs.iniobsahuje informace vztahující se ke všem správcům front v daném uzlu. Vytvoří se automaticky během instalace.

V systému IBM WebSphere MQ pro produkty UNIX and Linux jsou datové adresáře a adresář protokolu vždy `/var/mqm` a `/var/mqm/log` .

V systémech Windows jsou umístění datového adresáře `mqs.ini`a 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 souboru `mqinst.ini` v systému IBM WebSphere MQ pro systémy UNIX and 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\WepSphere MQ` . Obsahuje:

- Názvy správců front
- Název výchozího správce front
- Umístění souborů přidružených ke každému z nich

Dodaná sekce `LogDefaults` pro novou instalaci IBM WebSphere 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 `LogDefaults` v Obrázek 71 na stránce 409. Hodnota nula pro atribut `LogBufferPages` znamená 512.

Pokud požadujete jinou než výchozí hodnotu, musíte tuto hodnotu explicitně zadat ve stanze `LogDefaults` .

```
#*******************************************************************#
#* Module Name: mqs.ini                                            *#
#* Type       : WebSphere MQ Machine-wide Configuration File       *#
#* Function   : Define WebSphere 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 71. Příklad konfiguračního souboru IBM WebSphere MQ pro systémy UNIX

Konfigurační soubory správce front qm.ini

Konfigurační soubor správce front qm.iniobsahuje 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 7.5.0.9 V produktu IBM WebSphere MQ Version 7.5.0, opravná sada Fix Pack 9příkaz **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`

Windows Linux UNIX

V systémech UNIX and 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 zadáno položkou WorkPath , která je zadána v klíči HKLM\SOFTWARE\IBM\WebSphere MQ . Příklad: Cesta a název konfiguračního souboru pro správce front s názvem QMNAME je:

```
C:\Program Files\IBM\WebSphere 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 WebSphere MQ.

Příklad souboru qm.ini

Linux UNIX

Následující příklad ukazuje, jak mohou být skupiny atributů uspořádány v konfiguračním souboru správce front v produktu IBM WebSphere MQ pro systémy UNIX and Linux .

```
#* Module Name: qm.ini                                               *#
#* Type       : WebSphere 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=13

ServiceComponent:
   Service=AuthorizationService
   Name=MQSeries.UNIX.auth.service
   Module=opt/mqm/bin/amqzfu
   ComponentDataSize=0

Log:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0[1]
   LogPath=/var/mqm/log/saturn!queue!manager/

AccessMode:
   SecurityGroup=wmq\wmq

XAResourceManager:
   Name=DB2 Resource Manager Bank
   SwitchFile=/usr/bin/db2swit
   XAOpenString=MQBankDB
   XACloseString=
   ThreadOfControl=THREAD

Channels: [2]
   MaxChannels=200
   MaxActiveChannels=100
   MQIBindType=STANDARD
```

```
AccessMode:
   SecurityGroup=wmq\wmq
TCP:
   KeepAlive = Yes
   SvrSndBuffSize=32768
   SvrRcvBuffSize=32768
   Connect_Timeout=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
```

Notes:

1. Hodnota nula pro `LogBufferPages` udává hodnotu 512.
2. Další informace o sekci Kanál naleznete v tématu “Inicializační a konfigurační soubory” na stránce 68.
3. Maximální počet oddílů XAResourceManager je omezen na 255. Měli byste však použít pouze malý počet oddílů, abyste se vyvarovali snížení výkonu transakce.

Produkt WebSphere MQ v systému Unix používá konfigurační soubory, které mají příponu souboru .ini, například qm.ini. V produktu WebSphereMQ jsou některé obslužné programy, jako například **setmqm**, které vytvoří dočasnou záložní kopii souborů. Soubor qm.ini například vytvoří záložní kopii s názvem qm.ini.bak. Obslužný program upraví soubor qm.ini , uloží aktualizovaný soubor a poté odstraní soubor qm.ini.bak . Pokud obslužný program nemůže uložit soubor qm.ini , obnoví obsah souboru qm.ini ze záložního souboru qm.ini.baka pak odstraní soubor qm.ini.bak .

Existuje-li existující soubor qm.ini.bak , vrátí obslužný program soubor qm.ini obsahem souboru qm.ini.bak a odstraní soubor qm.ini.bak . Proto byste neměli vytvářet záložní kopie souborů *.ini pomocí přípony souboru .bak, protože tyto záložní soubory mohou být odstraněny obslužnými programy produktu WebSphere MQ .

Informace o tom, kdy se změny projeví, naleznete v příručce “Změna konfiguračních informací v systémech UNIX, Linux, and Windows” na stránce 406 .

Konfigurační soubor instalace mqinst.ini

Systémy UNIX and Linux

Konfigurační soubor instalace `mqinst.ini`obsahuje informace o všech instalacích produktu IBM WebSphere MQ v systému UNIX nebo Linux .

Soubor `mqinst.ini` se nachází v adresáři `/etc/opt/mqm` na systémech UNIX and 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.
dltmqinst k odstranění položek.

dspmqinst pro zobrazení položek.
setmqinst pro nastavení položek.

Je automaticky nastaven identifikátor instalace, pouze pro vnitřní použití, a nesmí být změněn.

Systémy Windows

Informace o konfiguraci instalace jsou uloženy v následujícím klíči na systémech Windows :

```
HKLM\SOFTWARE\IBM\WebSphere MQ\Installation\<InstallationName>
```

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 Windowsnejsou k dispozici příkazy **crtmqinst** a **dltmqinst** . Procesy instalace a odinstalace manipulují s vytvářením a odstraňováním požadovaných položek registru.

Atributy pro změnu konfiguračních informací IBM WebSphere MQ

V systému IBM WebSphere MQ pro systémy Windows a v systémech IBM WebSphere MQ for Linux (platformyx86 a x86-64) upravte informace o konfiguraci pomocí produktu IBM WebSphere MQ Explorer. V jiných systémech upravte informace úpravou konfiguračního souboru mqs.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 WebSphere MQ a správce front” na stránce 406
Změňte chování produktu IBM WebSphere MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související úlohy

Naplánování

Správa produktu WebSphere MQ

Související odkazy

“Změna konfiguračních informací správce front” na stránce 418
Zde popsané atributy upravují konfiguraci jednotlivého správce front. Přepisují veškerá nastavení pro produkt WebSphere MQ.

Všichni správci front

Použijte stránku vlastností `General` a `Extended` WebSphere MQ z Průzkumníka IBM WebSphere MQ nebo stanzu `AllQueueManagers` v souboru mqs.ini , abyste uvedli 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 produkt WebSphere MQ před změnou výchozí předpony a znovu spusťte produkt WebSphere MQ až poté, co přesunete struktury do nového umístění a změníte výchozí předponu.

Poznámka: Neodstraňujte adresář `/var/mqm/errors` v systémech UNIX and Linux nebo 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 určení způsobu, jakým má produkt WebSphere MQ převést znak NL EBCDIC do formátu ASCII.

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
Převeďte 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 části Tabulka 32 na stránce 413.

Tabulka 32. Seznam možných ISO CCSID

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.

Předvolený správce fronty

Pomocí stránky vlastností produktu `General` WebSphere MQ v Průzkumníku IBM WebSphere MQ nebo stanzy `DefaultQueueManager` v souboru mqs.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

Pomocí stránky vlastností produktu `Extended` IBM WebSphere MQ v Průzkumníku IBM WebSphere MQ nebo v souboru `ExitProperties` v souboru mqs.ini určete volby konfigurace používané ukončovacími 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 (amqzlwa0) 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 WebSphere MQ

Na stránce vlastností produktu `Default log settings` IBM WebSphere MQ v souboru IBM WebSphere MQ Explorernebo v souboru stanza `LogDefaults` v souboru mqs.ini můžete zadat 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** .

Po vytvoření správce front jsou atributy protokolu pro tohoto správce front převzaty z nastavení popsaných v tématu “Protokoly správce front” na stránce 422.

Výchozí předpona (určená v produktu “Všichni správci front” na stránce 412) a cesta k protokolu určená pro konkrétního správce front (zadané v produktu “Protokoly správce front” na stránce 422) umožňují správci front a jeho protokolu používat různé fyzické jednotky. Toto je doporučená metoda, ačkoli při výchozím nastavení jsou na stejné jednotce.

Informace o výpočtu velikosti protokolu viz “Výpočet velikosti protokolu” na stránce 391.

Poznámka: Limity uvedené v následujícím seznamu parametrů jsou limitními limity stanovenými produktem WebSphere MQ. Limity operačního systému mohou snížit maximální možnou velikost protokolu.

LogPrimaryFiles=3|*2-254* (Windows) |*2-510* (systémyUNIX and Linux)
Soubory protokolu přidělené při vytvoření správce front.

Minimální počet primárních souborů protokolu, které můžete mít, je 2 a maximum je 254 na systému Windows, nebo 510 na systémech UNIX and Linux . Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 na systémech UNIX and 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.

LogSecondaryFiles=2|*1-253* (Windows) |*1-509* (systémyUNIX and Linux)
Soubory protokolu přidělené při vyčerpání primárních souborů.

Minimální počet sekundárních souborů protokolu je 1 a maximum je 253 na systému Windows, nebo 509 na systémech UNIX and Linux . Výchozí hodnota je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 na systémech UNIX and 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 uchovávané 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.

Na systémech UNIX and 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
Spusťte zotavení restartováním pomocí protokolu k odvolání transakcí, které probíhaly, když se systém zastavil.

Podrobnější vysvětlení kruhového protokolování naleznete v části “Typy protokolování” na stránce 388 .

Lineární
Pro restartování obnovy a média nebo dopředné zotavení (vytváření ztracených nebo poškozených dat opětovným přehráváním obsahu protokolu).

Podrobnější vysvětlení lineárního protokolování najdete v části “Typy protokolování” na stránce 388 .

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.

LogBufferPages=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 produktu WebSphere MQ verze 7.0 je tato hodnota 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 produkt WebSphere MQ for Windows , kde `<DefaultPrefix>` je hodnota zadaná v atributu `DefaultPrefix` na stránce vlastností produktu `All Queue Managers` WebSphere MQ . Tato hodnota je nastavena při instalaci.
- `/var/mqm/log` pro systémy WebSphere MQ for UNIX and 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 mqs.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 atributech 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.

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
Volbu **SingleWrite** byste měli použít pouze, pokud systém souborů nebo zařízení hostující protokol zotavení pro produkt WebSphere MQ explicitně garantuje 4kB atomicitu pro zápis.

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.

rozhraní Advanced Configuration and Power Interface (ACPI)

Pomocí stránky vlastností produktu `ACPI` WebSphere MQ z Průzkumníka IBM WebSphere MQ můžete určit, jak se má produkt WebSphere MQ chovat, když systém obdrží požadavek na pozastavení.

Systém Windows podporuje standard ACPI (Advanced Configuration and Power Interface). To umožní uživatelům systému 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` WebSphere 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; přijměte 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 jsou zobrazeny v dialogovém okně (Poznámka; zamítnutí požadavku).

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 IBM WebSphere MQ Explorer nebo `amqmdain` .

Použijte stránku vlastností produktu `Exits` IBM WebSphere MQ ze souboru IBM WebSphere MQ Explorernebo sekci `ApiExitTemplate` a `ApiExitCommon` v souboru mqs.ini k identifikaci uživatelských procedur 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 stanzu `ApiExitLocal` , jak je popsáno v části “Uživatelské procedury rozhraní API” na stránce 431.)

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, UNIX and Linux existuje jedna 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 názvů naleznete v tématu Základní informace o názvech souborů produktu WebSphere 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 WebSphere 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 WebSphere MQ starší než verze 7.1.

Související pojmy

“Přidružení správce front k instalaci” na stránce 16
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **`crtmqm`** . V systému UNIX, Linux, and Windowsmůžete 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 produktu Windows.

Předvolba je nekontrolovat globální skupiny.

GlobalGroups
OAM kontroluje globální skupiny.

Pomocí sady `GlobalGroups` přijímají autorizační příkazy, **`setmqaut`**, **`dspmqaut`**a **`dmpmqaut`** globální názvy skupin, viz parametr **`setmqaut -g`**.

Poznámka: Nastavení produktu `ClusterQueueAcessControl=RQMName` a vlastní implementace autorizační služby na méně než `MQZAS_VERSION_6` výsledků ve správci front se nespouští. V této instanci buď nastavte `ClusterQueueAcessControl=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 produkt WebSphere MQ.

Na systémech UNIX and Linux upravíte informace o konfiguraci správce front úpravou konfiguračního souboru qm.ini . Definujete-li oddíl v souboru qm.ini, nemusíte každou položku spouštět na novém řádku. K označení komentáře můžete použít buď středník (;), nebo hašovací znak (#).

V systémech Windows a Linux (platformyx86 a x86-64) můžete upravit některé informace o konfiguraci pomocí produktu IBM WebSphere MQ Explorer. Avšak protože existují významné důsledky pro změnu instalovatelných služeb a jejich komponent, instalovatelné služby jsou jen pro čtení v IBM WebSphere MQ Explorer. Proto musíte provést jakékoli změny instalovatelných služeb pomocí produktu **regedit** v systému Windowsa úpravou souboru qm.ini na systému UNIX and 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 WebSphere MQ a správce front” na stránce 406
Změňte chování produktu IBM WebSphere MQ nebo jednotlivého správce front tak, aby vyhovovalo potřebám vaší instalace.

Související úlohy

Naplánování

Správa produktu WebSphere MQ

Související odkazy

“Atributy pro změnu konfiguračních informací IBM WebSphere MQ” na stránce 412
V systému IBM WebSphere MQ pro systémy Windows a v systémech IBM WebSphere MQ for Linux (platformyx86 a x86-64) upravte informace o konfiguraci pomocí produktu IBM WebSphere MQ Explorer. V jiných systémech upravte informace úpravou konfiguračního souboru mqs.ini .

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.

Použít skupinu přístupů (`-a [r]`) pomocí volby příkazu **crtmqm** určete skupinu zabezpečení systému Windows, jejímž členům bude 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 `-ar` 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` pro nastavení oprávnění ke složce, která obsahuje data a protokoly správce front. Na rozdíl od lokální skupiny `mqm` můžete další skupinu zabezpečení přístupu označit jako lokální nebo globální skupinu. 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, ID uživatele kontrolované systémem Windows je ID uživatele, které jste nakonfigurovali pomocí průvodce **Připravit** IBM WebSphere MQ . Pokud jste spustili správce front interaktivně, bude ID uživatele kontrolované systémem Windows ID uživatele, který spustil příkaz **strmqm**.

Chcete-li spustit správce front, musí být ID uživatele členem lokální skupiny mqm. 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 364

“Zabezpečit data správce sdílených front a adresáře a soubory protokolu v systému Windows” na stránce 361

Související úlohy

“Vytvoření správce front s více instancemi na pracovních stanicích nebo na serverech domény” na stránce 338

Související odkazy

crtmqm

Instalovatelné služby

Instalovatelné služby můžete změnit na Windows pomocí **regedit**, a na UNIX and Linux pomocí stanzy Service v souboru qm.ini .

Poznámka: Existují významné důsledky pro změnu instalovatelných služeb a jejich komponent. Z toho důvodu jsou instalovatelné služby určené pouze pro čtení v Průzkumníku WebSphere MQ .

Chcete-li změnit instalovatelné služby na systémech Windows , použijte regeditnebo na systémech UNIX and Linux , použijte sekci 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 UNIX and Linux použijte pro tento objekt stanza ServiceComponent .

Název =AuthorizationService|NameService
Název požadované služby.

AuthorizationService
Pro produkt WebSphere MQje komponenta Služba autorizace známá jako správce oprávnění k objektu nebo společnost 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.

SecurityPolicy=Default|NTSIDsRequired (pouze WebSphere MQ for Windows)
Atribut SecurityPolicy se použije pouze v případě, že uvedená služba je výchozí autorizační službou, to znamená 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 systému 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 najdete v tématu Identifikátory zabezpečení systémuWindows (SID) .

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, to znamená OAM. Atribut IsolatedBindingsUserId se používá pouze v případě izolovaných vazeb. 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 systémy UNIX, Linux a Windows.

Další informace o službách zabezpečení obecně najdete v tématu Nastavení zabezpečení v systémech Windows, UNIX and Linux.

Související odkazy
Referenční informace o instalovatelných službách

Servisní komponenty

Když přidáváte novou instalovatelnou službu, musíte uvést informace o komponentě služby. Na systémech Windows použijte `regedita` na systémech UNIX and 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 platné pro názvy objektů produktu WebSphere 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. Uveďte nulu, pokud nejsou požadována žádná data komponenty.

Další informace o instalovatelných službách a komponentách najdete v tématu Instalovatelné služby a komponenty pro systémy UNIX, Linux a Windows.

Protokoly správce front

Použijte stránku vlastností správce front produktu Log z Průzkumníka IBM WebSphere 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 WebSphere MQ” na stránce 414). 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 391.

Poznámka: Omezení uvedená v následujícím seznamu parametrů jsou nastavena produktem WebSphere MQ. Limity operačního systému mohou snížit maximální možnou velikost protokolu.

LogPrimarySoubory =3 |*2-254* (Windows) |*2-510* (systémyUNIX and Linux)
Soubory protokolu přidělené při vytvoření správce front.

Minimální počet primárních souborů protokolu, které můžete mít, je 2 a maximum je 254 na systému Windows, nebo 510 na systémech UNIX and Linux . Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 na systémech UNIX and 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* (systémyUNIX and Linux)
Soubory protokolu přidělené při vyčerpání primárních souborů.

Minimální počet sekundárních souborů protokolu je 1 a maximum je 253 na systému Windows, nebo 509 na systémech UNIX and Linux . Výchozí hodnota je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 na systémech UNIX and 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 uchovávané 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.

Na systémech UNIX and 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 WebSphere MQ” na stránce 414 .

CIRCULAR
Spusťte zotavení restartováním pomocí protokolu k odvolání transakcí, které probíhaly, když se systém zastavil.

Podrobnější vysvětlení kruhového protokolování naleznete v části “Typy protokolování” na stránce 388 .

Lineární
Pro restartování obnovy a média nebo dopředné zotavení (vytváření ztracených nebo poškozených dat opětovným přehráváním obsahu protokolu).

Podrobnější vysvětlení lineárního protokolování najdete v části “Typy protokolování” na stránce 388 .

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 produktu WebSphere MQ verze 7.0 je tato hodnota 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:\Program Files\IBM\WebSphere MQ\log` v příručce WebSphere MQ for Windows .
- `/var/mqm/log` v produktu WebSphere MQ pro systémy UNIX and 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 produktu WebSphere MQ pro systémy UNIX and Linux ID uživatele mqm a skupina mqm musí mít 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
Volbu **SingleWrite** byste měli použít pouze, pokud systém souborů nebo zařízení hostující protokol zotavení pro produkt WebSphere MQ explicitně garantuje 4kB atomicitu pro zápis.

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.

Omezený režim

Tato volba platí pouze pro systémy UNIX and 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 WebSphere 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 WebSphere 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 WebSphere MQ . Proto musíte také uživatelům udělit oprávnění pro připojení k produktu IBM WebSphere MQ a k přístupu k prostředkům, které vyžadují pomocí autorizační služby produktu IBM WebSphere MQ .

Windows Linux UNIX Další informace o konfiguraci autorizační služby produktu IBM WebSphere MQ lze nalézt v tématu Nastavení zabezpečení v systémech Windows, UNIX and Linux.

Omezený režim produktuIBM WebSphere 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 WebSphere MQ nebo sekci XA`ResourceManager` 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 atributech 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.

Produkt WebSphere MQ používá hodnotu `Name` ve zprávách a ve výstupu příkazu `dspmqtrn` .

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 informací o konfiguraci 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 informací o konfiguraci správce prostředků pro produkt Informix

a nahlédněte do dokumentace k databázi pro příslušný řetězec.

ThreadOfControl=THREAD |PROCESS
Tento atribut je povinný pro produkt WebSphere 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 WebSphere MQ lze volat funkci XA k externímu správci prostředků ve více podprocesech současně.

PROCESS
Správce prostředků není *bezpečný pro podproces*. Ve vícevláknovém procesu produktu WebSphere MQ 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 ve stanzách kanálů

Tyto atributy určují konfiguraci kanálu.

Tyto informace nejsou použitelné pro produkt WebSphere MQ pro platformu z/OS .

Chcete-li zadat informace o kanálech, použijte stránku vlastností správce front produktu `Channels` z Průzkumníka WebSphere 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 WebSphere MQ obdrží požadavek na spuštění kanálu, ale zjistí, že instance kanálu je již spuštěna, v některých případech musí být existující instance kanálu zastavena, než bude možné spustit nový. 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 AdoptNewMCATimout, 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 WebSphere 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.

Uveďte 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 hostbselže, 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`.

Související pojmy

“Stavy kanálů” na stránce 54
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, LU62, NETBIOS, a SPX

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 WebSphere 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. Číslo portu *dobře známé* pro produkt WebSphere MQ je 1414.

Library1 =*DLLName1* (pouze WebSphere 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 portu TCP/IP pro modul listener, aby přijal požadavek. Výchozí hodnoty nevyřízených požadavků modulu listener jsou zobrazeny v části Tabulka 33 na stránce 428.

Tabulka 33. Výchozí nevyřízené požadavky na připojení (TCP)

Platforma	**Výchozí hodnota ListenerBacklog**
Server Windows	100
Pracovní stanice Windows	5
Linux	100
Solaris	100
HP-UX	20
AIX V4.2 nebo novější	100
AIX V4.1 nebo starší	10

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 33 na stránce 428, 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.

SvrSndBuffSize=32768|number
Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá na konci serveru pro kanál připojení serveru připojení klienta.

SvrRcvBuffSize=32768|number
Velikost vyrovnávací paměti pro příjem protokolu TCP/IP v bajtech použitá na konci serveru kanálu připojení klienta pro připojení klienta k serveru.

Connect_Timeout=0|number
Počet sekund před pokusem o připojení k vypršení časového limitu soketu. Výchozí hodnota nula určuje, že časový limit připojení neexistuje.

LU62 (pouze WebSphere MQ for Windows)
Použijte stránku vlastností správce front produktu LU6.2 z Průzkumníka IBM WebSphere 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.

NETBIOS (pouze WebSphere MQ for Windows)
Použijte stránku vlastností správce front produktu `Netbios` z Průzkumníka IBM WebSphere 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_názvů*
Počet názvů, které se mají přidělit. Výchozí hodnota je 1.

Library1 =*DLLName1*
Název knihovny DLL NetBIOS .

Výchozí hodnota je NETAPI32.

SPX (pouze produkt WebSphere MQ for Windows)
Použijte stránku vlastností správce front produktu SPX z Průzkumníka IBM WebSphere 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. Může to být považováno za *nevyřízené požadavky* požadavků čekajících na soket SPX pro příjem požadavků na přijetí požadavku. Výchozí hodnoty nevyřízených požadavků modulu listener jsou zobrazeny v části Tabulka 34 na stránce 430.

Tabulka 34. Výchozí nevyřízené požadavky na připojení (SPX)

Platforma	**Výchozí hodnota ListenerBacklog**
Server Windows	100
Pracovní stanice Windows	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 34 na stránce 430, 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 WebSphere 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 IBM WebSphere 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 oddíly `ApiExitCommon` a `ApiExitTemplate` , jak je popsáno v tématu “Uživatelské procedury rozhraní API” na stránce 417.)

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 UNIX, Linux, and Windows

Použijte stránku vlastností správce front produktu `Extended` z Průzkumníka produktu WebSphere MQ nebo sekci `QMErrorLog` v souboru qm.ini , abyste přizpůsobili operaci a obsah protokolů chyb správce front.

Upozornění: K provedení změn můžete použít produkt WebSphere 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 WebSphere MQ intenzivně využíván, je při zastavování a spouštění mnoha kanálů odesláno velké množství informačních zpráv do konzoly z/OS a do protokolu hardcopy. Most WebSphere MQ-IMS a správce vyrovnávací paměti mohou také produkovat velké množství informačních zpráv, takže vyloučení zpráv vám zabrání v příjmu velkého počtu zpráv, pokud jej požadujete. *msqIds* 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.
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.
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 WebSphere MQ intenzivně využíván, je při zastavování a spouštění mnoha kanálů odesláno velké množství informačních zpráv do konzoly z/OS a do protokolu hardcopy. Most WebSphere MQ-IMS a správce vyrovnávací paměti mohou také produkovat velké množství informačních zpráv, takže potlačením zpráv zabráníte v příjmu několika opakujících se zpráv, pokud to požadujete. Časový interval je určen parametrem `SuppressInterval`. *msqIds* 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.
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.
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 WebSphere MQ nebo stanzu `Connection` v souboru qm.ini , abyste určili výchozí typ vazby.

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.

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. Nezapíší 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.

- ANO: Kanály SSL nebo TLS se snaží zkontrolovat servery CDP za účelem určení, zda je digitální certifikát odvolán.
- NO: Kanály SSL nebo TLS se nesnažte kontrolovat servery CDP. Tato hodnota je výchozí.

OCSPAuthentication=REQUIRED|WARN|OPTIONAL

OCSPAuthentication 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 OCSPAuthentication.

- 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.

- ANO: Kanály SSL a TLS se snaží zkontrolovat servery OCSP, aby určily, zda je digitální certifikát odvolán. Tato hodnota je výchozí.
- NO: 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 v systému AIXmůže 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 odpovídacího modulu OCSP.

Vlastnosti uživatelské procedury

Chcete-li zadat informace o vlastnostech ukončení ve správci front, použijte stránku vlastností správce front klastru z produktu IBM WebSphere 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 414). 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
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 (amqzlwa0) 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.

Podfond

Tato stanza je vytvořena produktem WebSphere MQ. Neměňte jej.

Když vytváříte správce front, jsou WebSphere MQ při vytváření správce front automaticky zapisovány do oddílu podfondu a v atributu ShortSubpoolnázev v rámci této stanzy. Produkt WebSphere MQ vybere hodnotu pro název ShortSubpool. Tuto hodnotu neměňte.

Tento název odpovídá adresáři a symbolickému odkazu vytvořenému v adresáři /var/mqm/sockets , který produkt WebSphere MQ používá pro interní komunikaci mezi spuštěnými procesy.

KonfiguraceHP Integrity NonStop Server

Tyto informace vám pomohou při konfiguraci vašeho klienta IBM WebSphere MQ pro instalaci produktu HP Integrity NonStop Server .

Podrobnosti o konfiguraci klienta pomocí konfiguračního souboru viz “Konfigurace klienta pomocí konfiguračního souboru” na stránce 123.

Podrobnosti o konfiguraci klienta pomocí proměnných prostředí naleznete v tématu “Použití proměnných prostředí produktu WebSphere MQ” na stránce 141.

Pokud provádíte klienta IBM WebSphere MQ 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, abyste umožnili klientovi IBM WebSphere MQ pro produkt HP Integrity NonStop Server přístup k bráně TMF Gateway.

Tato sekce obsahuje také klienta IBM WebSphere MQ pro HP Integrity NonStop Server specifické informace o udělení oprávnění pro kanály.

Přehled procesu brány

Produkt HP NonStop Transaction Management Facility (TMF) poskytuje služby, které umožňují procesu brány zaregistrovat se jako správce prostředků. IBM WebSphere MQ poskytuje proces TMF/Gateway spuštěný pod cestou Pathway.

IBM WebSphere MQ registruje jeden proces brány pro každého správce front, který je koordinován TMF, proto musíte nakonfigurovat samostatný TMF/Gateway pro každého správce front, který se má 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 srozuminém mapování.

V případě více instalací produktu IBM WebSphere MQmusíte 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 WebSphere MQ , které umožňuje TMF být koordinátorem transakcí pro transakce IBM WebSphere MQ .

Produkt IBM WebSphere MQ poskytuje TMF/Gateway konvertuje transakce z koordinace TMF do koordinace transakcí architektury eXtended Architecture (XA) pro komunikaci se vzdáleným správcem front.

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 mechanizmy 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 0SS.

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 WebSphere MQ , a proto tento atribut musí být nastaven na 0N.

PROGRAM=<OSS installation path>/opt/mqm/bin/runmqtmf
Pro klienta IBM WebSphere MQ for IBM WebSphere MQmusí 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 -h` jako alternativní způsob poskytování informací o připojení ke komunikační bráně spolu s informacemi popsanými v příručce “Konfigurace TMF/Gateway pomocí proměnných prostředí” na stránce 437. Pokud uvedete jeden nebo více, ale ne všechny atributy `-c`, `-pa -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 WebSphere MQ .

`LINKDEPTH` a `MAXLINKS` musí být nakonfigurovány s hodnotami vhodnými pro očekávaný počet klientských aplikací IBM WebSphere MQ , které mohou chtít souběžně komunikovat s bránou Gateway. Jsou-li tyto hodnoty nastaveny příliš nízko, mohou se zobrazit výskyty chybové zprávy AMQ5399 vydané z klientských aplikací.

Další informace o těchto atributech 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 WebSphere MQ , abyste umožnili klientovi IBM WebSphere MQ pro přístup HP Integrity NonStop Server k bráně TMF Gateway.

Inicializační soubor klienta IBM WebSphere MQ pro HP Integrity NonStop Server lze zadržet v řadě lokalit, abyste získali další informace, viz “Umístění konfiguračního souboru klienta” na stránce 124.

Podrobné informace o obsahu konfiguračního souboru společně s příkladem viz “Konfigurace klienta pomocí konfiguračního souboru” na stránce 123. Použijte sekci TMF k určení správce front TMF a podrobnosti o serveru, abyste získali další informace, prohlédněte si téma “stanza TMF a TMF/Gateway” na stránce 141.

Příklad položek pro klienta IBM WebSphere 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 produktu WebSphere MQ” na stránce 141.

Udělení oprávnění pro kanály

Udělení oprávnění k kanálům na klientovi IBM WebSphere 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.

Použijte příkaz **setmqaut** k udělení autorizace, to znamená, že poskytnu oprávnění uživatele IBM WebSphere MQ nebo skupiny uživatelů k provedení operace a zrušení autorizace, to znamená odebrání oprávnění k provedení operace.

Poznámky

Tyto informace byly vyvinuty pro produkty a služby poskytované v USA.

Společnost IBM nemusí nabízet produkty, služby nebo funkce uvedené v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou ve vaší oblasti aktuálně dostupné, získáte od místního zástupce společnosti IBM. Odkazy na produkty, programy nebo služby společnosti IBM v této publikaci nejsou míněny jako vyjádření nutnosti použití pouze uvedených produktů, programů či služeb společnosti IBM. Místo toho lze použít jakýkoli funkčně ekvivalentní produkt, program nebo službu, které neporušují žádná práva k duševnímu vlastnictví IBM. Ověření funkčnosti produktu, programu nebo služby pocházející od jiného výrobce je však povinností uživatele.

Společnost IBM může vlastnit patenty nebo nevyřízené žádosti o patenty zahrnující předměty popsané v tomto dokumentu. Vlastnictví tohoto dokumentu neposkytuje licenci k těmto patentům. Dotazy týkající se licencí můžete posílat písemně na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Odpovědi na dotazy týkající se licencí pro dvoubajtové znakové sady (DBCS) získáte od oddělení IBM Intellectual Property Department ve vaší zemi, nebo tyto dotazy můžete zasílat písemně na adresu:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE" , BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás toto omezení nemusí vztahovat.

Uvedené údaje mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené jsou pravidelně upravovány a tyto změny budou zahrnuty v nových vydáních této publikace. Společnost IBM může kdykoli bez upozornění provádět vylepšení nebo změny v produktech či programech popsaných v této publikaci.

Veškeré uvedené odkazy na webové stránky, které nespravuje společnost IBM, jsou uváděny pouze pro referenci a v žádném případě neslouží jako záruka funkčnosti těchto webů. Materiály uvedené na tomto webu nejsou součástí materiálů pro tento produkt IBM a použití uvedených stránek je pouze na vlastní nebezpečí.

Společnost IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vyžádání vašeho svolení.

Vlastníci licence k tomuto programu, kteří chtějí získat informace o možnostech (i) výměny informací s nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) oboustranného využití vyměňovaných informací, mohou kontaktovat informační středisko na adrese:

IBM Corporation
Koordinátor spolupráce softwaru, oddělení 49XA
148 00 Praha 4-Chodby

148 00 Praha 4-Chodov
U.S.A.

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek smlouvy IBM Customer Agreement, IBM International Program License Agreement nebo jiné ekvivalentní smlouvy mezi námi.

Jakékoli údaje o výkonnosti obsažené v této publikaci byly zjištěny v řízeném prostředí. Výsledky získané v jakémkoli jiném operačním prostředí se proto mohou výrazně lišit. Některá měření mohla být prováděna na vývojových verzích systémů a není zaručeno, že tato měření budou stejná i na běžně dostupných systémech. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky mohou být jiné. Čtenáři tohoto dokumentu by měli zjistit použitelné údaje pro své specifické prostředí.

Informace týkající se produktů jiných výrobců pocházejí od dodavatelů těchto produktů, z jejich veřejných oznámení nebo z jiných veřejně dostupných zdrojů. Společnost IBM tyto produkty netestovala a nemůže potvrdit správný výkon, kompatibilitu ani žádné jiné výroky týkající se produktů jiných výrobců než IBM. Otázky týkající se kompatibility produktů jiných výrobců by měly být směrovány dodavatelům těchto produktů.

Veškerá tvrzení týkající se budoucího směru vývoje nebo záměrů společnosti IBM se mohou bez upozornění změnit nebo mohou být zrušena a reprezentují pouze cíle a plány společnosti.

Tyto údaje obsahují příklady dat a sestav používaných v běžných obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob a názvy společností, značek a produktů. Všechna tato jména a názvy jsou fiktivní a jejich podobnost se jmény, názvy a adresami používanými ve skutečnosti je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly plně testovány za všech podmínek. Společnost IBM proto nemůže zaručit spolehlivost, upotřebitelnost nebo funkčnost těchto programů.

Při prohlížení těchto dokumentů v elektronické podobě se nemusí zobrazit všechny fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Informace programátorských rozhraní, je-li poskytnuta, vám pomohou vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, které umožňují zákazníkům psát programy za účelem získání služeb produktu IBM WebSphere MQ.

Tyto informace však mohou obsahovat i diagnostické údaje a informace o úpravách a ladění. Informace o diagnostice, úpravách a vyladění jsou poskytovány jako podpora ladění softwarových aplikací.

Důležité: Nepoužívejte tyto informace o diagnostice, úpravách a ladění jako programátorské rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM , ibm.comjsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek IBM je k dispozici na webu na stránce "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Ostatní názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností.

Microsoft a Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Tento produkt obsahuje software vyvinutý v rámci projektu Eclipse Project (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: